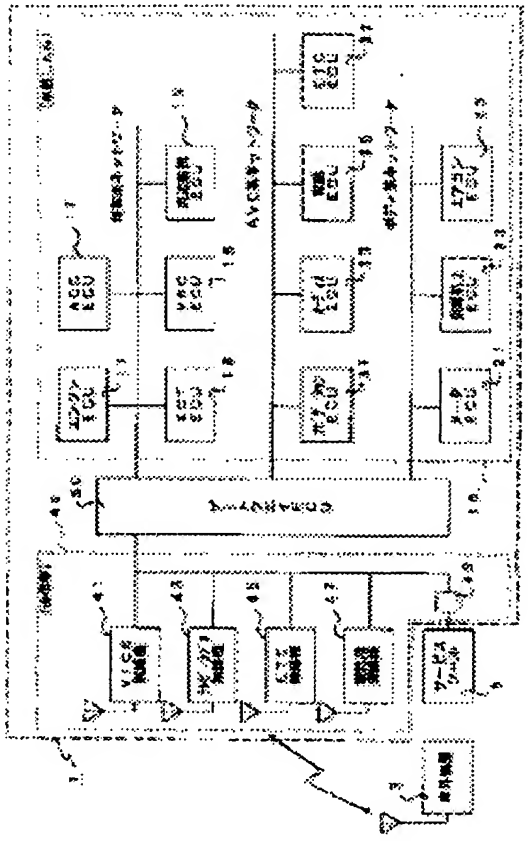
VEHICLE USE RELAY DEVICE AND IN-VEHICLE COMMUNICATION SYSTEM

Publication number: JP2003046536
Publication date: 2003-02-14
Inventor: AKIYAMA SUSUMU
Applicant: DENSO CORP
Classification:
- international: ***H04L12/40; H04L12/28; H04L12/46;*** **H04L12/40; H04L12/28; H04L12/46;** (IPC1-7): H04L12/46; H04L12/28; H04L12/40
- European:
Application number: JP20010231673 20010731
Priority number(s): JP20010231673 20010731

Abstract of **JP2003046536**

PROBLEM TO BE SOLVED: To sufficiently prevent various in-vehicle electric devices from being unauthorizedly accessed from the outside, while simplifying wiring of an in-vehicle communication system. SOLUTION: The in-vehicle communication system 1 comprises an on-vehicle LAN 10 to which ECUs 11 to 37 in a vehicle are connected, a communication section 40 for communication with an out-vehicle device 3, and a gateway ECU 5 that is placed in between the on-vehicle LAN and the communication section and relays data communication. The gateway ECU authenticates the out-vehicle device, when write request for a program from the out-vehicle device to an ECU in the on-vehicle LAN via the communication section and enables the ECU being a program write object ECU to authenticate the out-vehicle device. Furthermore, the gateway ECU in the case of receiving communication data other than the program write request authenticates the out-vehicle device by itself, when discriminating the data are not destinated to the ECUs 31 to 37 of an AVC system network.



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-046536

(43)Date of publication of application : 14.02.2003

(51)Int.Cl. H04L 12/46
H04L 12/28
H04L 12/40

(21)Application number : 2001-231673

(22)Date of filing : 31.07.2001

(71)Applicant : DENSO CORP

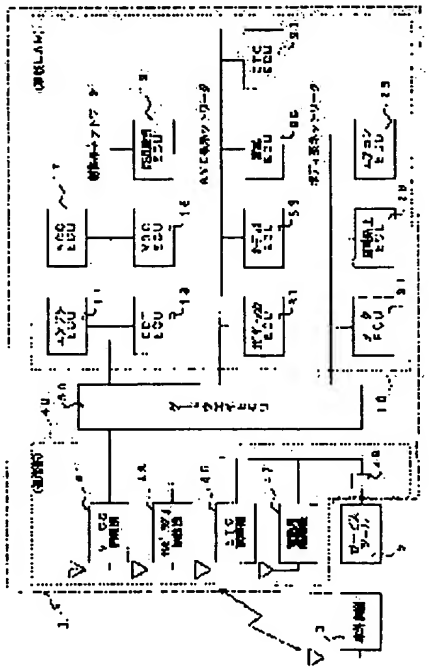
(72)Inventor : AKIYAMA SUSUMU

(54) VEHICLE USE RELAY DEVICE AND IN-VEHICLE COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To sufficiently prevent various in-vehicle electric devices from being unauthorizedly accessed from the outside, while simplifying wiring of an in- vehicle communication system.

SOLUTION: The in-vehicle communication system 1 comprises an on-vehicle LAN 10 to which ECUs 11 to 37 in a vehicle are connected, a communication section 40 for communication with an out-vehicle device 3, and a gateway ECU 5 that is placed in between the on-vehicle LAN and the communication section and relays data communication. The gateway ECU authenticates the out-vehicle device, when write request for a program from the out-vehicle device to an ECU in the on-vehicle LAN via the communication section and enables the ECU being a program write object ECU to authenticate the out-vehicle device. Furthermore, the gateway ECU in the case of receiving communication data other than the program write request authenticates the out-vehicle device by itself, when discriminating the data are not destinated to the ECUs 31 to 37 of an AVC system network.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]Repeating installation for vehicles characterized by comprising the following. Mounted LAN built by vehicles.
It is the repeating installation for vehicles which relays communication between various electronic devices in vehicles connected with a device outside a vehicle which is arranged between communication apparatus which perform data communications between devices outside a vehicle, and is connected via this communication apparatus at mounted LAN, If there is an access request from a device outside a vehicle to an electronic device in vehicles in said mounted LAN, will identify the access point, and. The first identification device that judges whether it is an access request to an electronic device in said vehicles for which this access request needs attestation of a device outside a vehicle based on this discriminated result, If said first identification device judges said access request to be what needs attestation of a device outside said vehicle, The first authentication means that judges whether a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand based on the first certification information transmitted from a device outside said vehicle, This first authentication means. [whether a device outside said vehicle which has carried out the access request is judged to be the device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand, and] If said first identification device judges said access request to be what does not need attestation of a device outside said vehicle, commo data transmitted via said communication apparatus from a device outside said vehicle, The first distribution means distributed to an electronic device in said vehicles of an access point.

[Claim 2]An information system device for reporting information acquired from the exterior as an electronic device in said vehicles in said mounted LAN to a vehicle occupant, ** is connected with control system equipment for controlling vehicles, and said first identification device, If there is an access request to an electronic device in said vehicles,

this access request by identifying whether it is which access request of said information system device and said control system equipment, This access request judges whether it is an access request to an electronic device in said vehicles which needs attestation of a device outside said vehicle, and said first authentication means, If said first identification device judges said access request to be an access request to said control system equipment, The repeating installation for vehicles according to claim 1 judging whether a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand based on the first certification information transmitted from a device outside said vehicle.

[Claim 3]When there is an access request from a device outside said vehicle to an electronic device in said vehicles, this access request, The second identification device that judges whether it is a write request for writing in a parameter a program which operates with an electronic device in vehicles, or for electronic device operation in vehicles, If said second identification device judges an access request to an electronic device in said vehicles not to be said write request, Operate said first identification device, and if said second identification device judges an access request to an electronic device in said vehicles to be said write request, Based on the second transmitted certification information, from a device outside said vehicle, a device outside said vehicle which has carried out the write request, The second authentication means that judges whether it is the device outside a vehicle to which writing of a parameter a program which operates with an electronic device in said vehicles, or for said electronic device operation in vehicles was permitted, Only when it is judged that this second authentication means is the device outside a vehicle to which writing of a parameter a program which operates a device outside said vehicle which has carried out the write request with an electronic device in said vehicles, or for said electronic device operation in vehicles was permitted, The second distribution means that distributes commo data transmitted via said communication apparatus from this device outside a vehicle to an electronic device in said vehicles of an access point, The repeating installation for vehicles according to claim 1 or 2 characterized by preparation ******.

[Claim 4]If said second identification device judges an access request to an electronic device in said vehicles to be said write request, said second authentication means, If it judges whether a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand based on said first certification information and a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand, The repeating installation for vehicles according to claim 3 judging whether a device outside said vehicle which has carried out the write request is a device outside a vehicle to which writing of a parameter a program which operates with an electronic device in said vehicles, or for said electronic device operation in vehicles was permitted based on said second certification information.

[Claim 5]Said second authentication means by comparing said first certification information

transmitted from a device outside said vehicle with certification information which self owns, If it judges whether a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand and a device outside said vehicle is a device outside a vehicle to which access to an electronic device in said vehicles was permitted beforehand, Said second certification information transmitted from a device outside said vehicle is transmitted to an electronic device in said vehicles used as a write object of said program or said parameter, Make this electronic device in vehicles compare said second certification information with certification information which this electronic device in vehicles owns, and. Acquire this collated result from this electronic device in vehicles, and based on a this acquired collated result, The repeating installation for vehicles according to claim 4 judging whether a device outside said vehicle which has carried out the write request is a device outside a vehicle to which writing of a parameter a program which operates with an electronic device in said vehicles, or for said electronic device operation in vehicles was permitted.

[Claim 6]A communications system comprising in the car:

Mounted LAN built by vehicles.

A communication apparatus which performs data communications between devices outside a vehicle.

This communication apparatus.

The repeating installation for vehicles according to any one of claims 1 to 5 which relays communication between various electronic devices in vehicles connected with a device outside a vehicle which is arranged between said mounted LAN and connected via said communication apparatus at said mounted LAN.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the repeating installation for vehicles which relays communication between the device outside a vehicle connected via a communication apparatus, and the various electronic devices in vehicles connected to mounted LAN.
[0002]
[Description of the Prior Art]In vehicles in recent years, especially a car, a control device, information machines and equipment, audio equipment, The number of loading of the said various electronic devices in vehicles is increasing, and about the electronic device in vehicles the coordinated movements between devices or sharing of information. It is common to connect by a communication wire for exclusive use, and to build the network for information and telecommunications (what is called mounted LAN) so that information can be transmitted and received between [each] devices.
[0003]It follows on the network besides vehicles having progressed in recent years, The infrastructure which can acquire a variety of information required for each device in vehicles from the outside of vehicles is fixed, and the example which connects many electronic devices in vehicles provided with the walkie-talkie for communicating between the devices outside a vehicle to mounted LAN is increasing in connection with this.
[0004]For example, a navigation device which can connect the cellular phone etc. which are used for the purpose of collecting neighboring store information from the Internet of a VICS walkie-talkie or the exterior which can receive the road traffic information provided from a vehicle information communication system (VICS), It is the on-board ETC unit etc. to which the ETC walkie-talkie for communicating between automatic fee accounting systems (ETC) was connected.
[0005]
[Problem(s) to be Solved by the Invention]However, in the conventional mounted LAN, Since it had become the composition which carries out direct continuation to the mainly

used apparatus about the information in the walkie-talkie for acquiring a variety of information from the exterior, it has not arranged in the position of a request in the car, and the walkie-talkie had to carry out excessive wiring between a walkie-talkie and apparatus, and was inconvenient.

[0006]In order to cancel this problem, direct continuation of the walkie-talkie is carried out to mounted LAN, and how the device in mounted LAN which needs the information which the walkie-talkie received enables it to acquire required information from a walkie-talkie via that mounted LAN can be considered, for example. If it does in this way, it will be high, and also there will also be few wiring numbers, and the flexibility of the installed position of a walkie-talkie etc. will be settled convenience.

[0007]However, it becomes possible to access each device connected to mounted LAN from the outside of vehicles via the walkie-talkie as it is such composition, and a possibility that the same problem as unlawful access to the network terminal which occur frequently in fields, such as the Internet, will occur is high in recent years.

[0008]This invention is made in view of such a problem, and an object [simplifying the wiring in a communications system in the car] of this invention is to fully prevent unlawful access from the outside to the various electronic devices in vehicles in vehicles.

[0009]

[Means for Solving the Problem]In the invention according to claim 1 made in order to attain this purpose, It is arranged between mounted LAN built by vehicles and a communication apparatus which performs data communications between devices outside a vehicle, Repeating installation for vehicles which relays communication between various electronic devices in vehicles connected with a device outside a vehicle connected via the communication apparatus at mounted LAN is equipped with the first identification device, the first authentication means, the first distribution means, and **.

[0010]Namely, if repeating installation for vehicles of this invention has an access request to an electronic device in vehicles connected to mounted LAN from a device outside a vehicle, will identify the access point in the first identification device, and. Based on the discriminated result, an access request judges whether it is an access request to an electronic device in vehicles which needs attestation of a device outside a vehicle.

[0011]If the first identification device judges the access request to be what needs attestation of a device outside a vehicle, repeating installation for vehicles, Based on the first certification information transmitted from a device outside a vehicle in the first authentication means, it is judged whether a device outside a vehicle is a device outside a vehicle to which access to an electronic device in vehicles was permitted beforehand.

[0012]repeating installation for vehicles, when a device outside a vehicle in which the first authentication means has carried out the access request is judged to be the device outside a vehicle to which access to an electronic device in vehicles was permitted beforehand, When the first identification device judges an access request to be what does not need attestation of a device outside a vehicle, commo data transmitted via a communication

apparatus in the first distribution means from a device outside a vehicle is distributed to an electronic device in vehicles of an access point.

[0013]Therefore, the repeating installation for vehicles according to claim 1 can refuse access to an electronic device in the vehicles about access from a device outside a vehicle with which access to an electronic device in vehicles in mounted LAN is not permitted, before connecting a device outside a vehicle to mounted LAN. if it puts in another way, the repeating installation for vehicles can restrict access from the outside by attesting a device outside a vehicle by the first authentication means -- a result -- the exterior -- unlawful access can be prevented.

[0014]As a method of making it judging whether it is an access request to an electronic device in vehicles with which an access request needs attestation of a device outside a vehicle for the first identification device, For example, an electronic device in vehicles which needs attestation of a device outside a vehicle in repeating installation for vehicles is listed beforehand, and there is a method of making it judge whether, based on the list, attestation of a device outside a vehicle is needed for the first identification device. In addition, two or more independent networks are built according to a system of an electronic device in vehicles as mounted LAN, If repeating installation for vehicles is not passed at these networks, it prevents from accessing from the outside, It may be made to judge whether it is that to which an access request needs attestation of a device outside a vehicle for the first identification device when an access request makes it judge whether it is an access request to an electronic device in vehicles belonging to a network of which system.

[0015]Certification information (password etc.) for every electronic device in vehicles is beforehand stored in repeating installation for vehicles, and authentication methods in case attestation of a device outside a vehicle is needed in this case include a method of making that certification information and certification information acquired from a device outside a vehicle compare with repeating installation for vehicles, for example. When certification information common to an electronic device in vehicles is stored in repeating installation for vehicles as another example and there is an access request [need / a device outside a vehicle / to be attested], a device outside a vehicle may be made to attest in common certification information regardless of an access point.

[0016]In addition, an information system device for reporting information which acquired an electronic device in vehicles connected to mounted LAN from the exterior to a vehicle occupant, It may be made to judge, when it classifies into control system equipment for controlling vehicles and an access request makes the first identification device identify which access request it is among an information system device and control system equipment whether attestation of a device outside a vehicle is necessity.

[0017]In this case, when [according to claim 2] the first identification device judges an access request to be an access request to control system equipment like, it is good to constitute repeating installation for vehicles so that the first recognition means may attest a device outside a vehicle with a described method.

[0018]Thus, if it sets, control system equipment for controlling vehicles can be accessed only from a just device outside a vehicle which received attestation, and the repeating installation for vehicles can prevent unlawful access to control system equipment concerning a run of vehicles. By the way, although the technique of judging whether a device outside a vehicle needs to be attested by above identifying an access point was taken, also when it is better to attest a device outside a vehicle irrespective of an access point depending on kinds (kind of commo data, etc.) of access request from a device outside a vehicle, it thinks.

[0019]For example, access requests are a program which operates with an electronic device in vehicles, a case where it is a write request for writing in a parameter for electronic device operation in vehicles (for example, conformity constant for operating a control system in vehicles exactly), etc. For this reason, in addition to the first identification device, the first authentication means, and the first distribution means, in the repeating installation for vehicles according to claim 3, the second identification device, the second authentication means, and the second distribution means are established.

[0020]Namely, if the repeating installation for vehicles according to claim 3 has an access request to device empty vehicle both [outside a vehicle] inner electronic device, It is judged whether it is a write request for the access request to write in a parameter a program which operates with an electronic device in vehicles, or for electronic device operation in vehicles in the second identification device, If the second identification device judges an access request to an electronic device in vehicles not to be a write request, the second authentication means is made composition which operates the first identification device.

[0021]If an access request to an electronic device in vehicles is judged to be a write request of a parameter for a program or electronic device operation in vehicles, the second identification device this repeating installation for vehicles, Based on the second certification information transmitted from a device outside a vehicle, it is judged whether a device outside a vehicle which has carried out the write request in the second authentication means is a device outside a vehicle to which writing of a parameter a program which operates with an electronic device in vehicles, or for electronic device operation in vehicles was permitted.

[0022]And only when it is judged that it is the device outside a vehicle to which writing of a parameter a program which operates a device outside a vehicle in which the second authentication means has carried out the write request with an electronic device in vehicles, or for electronic device operation in vehicles was permitted, A parameter a program as commo data transmitted via a communication apparatus in the second distribution means from a device outside a vehicle or for electronic device operation in vehicles is distributed to an electronic device in vehicles of an access point.

[0023]Therefore, in the repeating installation for vehicles according to claim 3, When an access request is a write request of a parameter for a program or electronic device

operation in vehicles, Regardless of an access point, based on the second certification information, a device outside a vehicle can be attested and a program to a result and an electronic device in vehicles by unjust access and writing of a parameter for electronic device operation in vehicles can be prevented.

[0024]Of course, when it is a write request from a just device outside a vehicle. Since it is a mechanism in which a parameter for a program or electronic device operation in vehicles is distributed to an electronic device in vehicles of an access point in the second distribution means, A valid user can be made to write in and update a program of an electronic device in vehicles, and a parameter for electronic device operation in vehicles simply according to the repeating installation for vehicles concerned, preventing writing of a parameter a program by unlawful access, and for electronic device operation in vehicles.

[0025]For example, in the former, although a dealer etc. were making a program of an electronic device in vehicles update by apparatus for exclusive use, a program can be updated, without forcing upon a driver etc. a troublesome thing [a thing] vehicles are carried in at a dealer in vehicles with which such repeating installation for vehicles was incorporated.

[0026]In the repeating installation for vehicles according to claim 3, it is desirable to adopt a firm authentic method which can judge whether a device outside a vehicle is more certainly just in an authentic method when an access request is the writing of a parameter for a program or electronic device operation in vehicles.

[0027]for this reason -- being alike -- for example -- being according to claim 4, if the second identification device judges an access request to an electronic device in vehicles to be a write request like, If the second authentication means judges whether a device outside a vehicle is a device outside a vehicle to which access to an electronic device in vehicles was permitted beforehand based on the first certification information and a device outside a vehicle is a device outside a vehicle to which access to an electronic device in vehicles was permitted beforehand, It is good to constitute repeating installation for vehicles so that it may judge whether a device outside a vehicle which has carried out the write request is a device outside a vehicle to which writing of a parameter a program which operates with an electronic device in vehicles, or for electronic device operation in vehicles was permitted based on the second certification information.

[0028]Thus, since a device outside a vehicle can be attested in two steps based on the first certification information and second certification information if repeating installation for vehicles is constituted, it can be distinguished more certainly whether a program and a write request of a parameter for electronic device operation in vehicles are the things from a just device outside a vehicle. Therefore, according to repeating installation for vehicles of this invention (claim 4), unlawful access to an electronic device in vehicles connected to mounted LAN can be prevented more certainly.

[0029]Specifically, it is preferred according to claim 5 to constitute the repeating installation for vehicles according to claim 4 like. By comparing the first certification information that

owns certification information for the second authentication means to attest a device outside a vehicle in the repeating installation for vehicles according to claim 5, and has been transmitted from a device outside a vehicle with the certification information which self owns, It is constituted so that it may judge whether a device outside a vehicle is a device outside a vehicle to which access to an electronic device in vehicles was permitted beforehand.

[0030]If it judges that this second authentication means is the device outside a vehicle with which a device outside a vehicle was permitted beforehand access to an electronic device in vehicles, the second certification information transmitted from a device outside a vehicle will be transmitted to an electronic device in vehicles used as a write object of a parameter for a program or electronic device operation in vehicles.

[0031]To an electronic device in vehicles which receives this second transmitted certification information. Certification information for judging whether a device outside a vehicle is a device outside a vehicle to which writing of a parameter for a program or electronic device operation in vehicles was permitted is memorized, and the second authentication means, An electronic device in vehicles is made to compare the second certification information with certification information which an electronic device in the vehicles owns by transmitting the second certification information. It is judged whether a device outside a vehicle which acquired the collated result from an electronic device in vehicles, and has carried out the write request based on an acquired collated result is a device outside a vehicle to which writing of a parameter a program which operates with an electronic device in vehicles, or for electronic device operation in vehicles was permitted.

[0032]In the repeating installation for vehicles according to claim 5 which attests a device outside a vehicle with such an authentication method. Since the second attestation is made to perform to the program or an electronic device in vehicles of a write object of a parameter, when repeating installation for vehicles should malfunction by unlawful access, an unjust program and writing of a parameter for electronic device operation in vehicles can be prevented. A device can be directly connected to mounted LAN and it can be prevented also to an act which is going to access unlawfully to an electronic device in vehicles.

[0033]If the repeating installation for vehicles according to any one of claims 1 to 5 explained above is used, a communications system in the car which is equal to unlawful access can be built. Specifically The communication apparatus according to claim 6 which performs data communications for the repeating installation for vehicles according to any one of claims 1 to 5 between devices outside a vehicle like, What is necessary is to arrange between mounted LAN built by vehicles and just to make communication between various electronic devices in vehicles connected with a device outside a vehicle connected to the repeating installation for vehicles via a communication apparatus at mounted LAN relay.

[0034]Under the present circumstances, if all the communication apparatus carried in vehicles are connected to repeating installation for vehicles, repeating installation for vehicles can relay all accesses from a device outside a vehicle, and all unlawful accesses

can be made to cope with it with repeating installation for vehicles. Therefore, in such a communications system in the car, unlawful access to an electronic device in vehicles can be prevented more certainly.

[0035]

[Embodiment of the Invention]The example of this invention is described with a drawing below. Drawing 1 is a block diagram showing the composition of the communications system 1 in the car with which this invention was applied.

[0036]As shown in drawing 1, the communications system 1 of this example in the car, Mounted LAN10 built by each electronic control (ECUs 11-37) installed in vehicles as an electronic device in vehicles, It is arranged between the communications department 40 for communicating between the devices 3 outside a vehicle, mounted LAN10, and the communications department 40, and is ** constituted with gateway ECU50 which relays the data communications between each ECUs 11-37 in mounted LAN10, and the device 3 outside a vehicle.

[0037]The above-mentioned ECU in the vehicles corresponding to each system is connected to the transmission line with the above-mentioned mounted LAN10 [common to a control system network, an AVC system network, a body system network, and each network, ** and others,] built in vehicles. For example, ECU for vehicle control concerning a run of engine ECU11, ECT-ECU13, VSC-ECU15, ACC-ECU17, and circumference surveillance ECU19 grade is connected to the control system network.

[0038]Engine ECU11 is an engine control system which controls an engine here, ECT-ECU13 is a speed change controlling device which performs transmission control of an automatic transmission, and these are the so-called control devices of a power-train system. VSC-ECU15 is a control device which performs the attitude control and braking control of vehicles, ACC-ECU17 is a running control device which performs control in which vehicles are made to follow precedence vehicles, and these are the so-called control devices of a vehicle motion system.

[0039]On the other hand, ECU for body control of meter ECU21, anti-theft ECU23, and air-conditioner ECU25 grade is connected to the body system network. Meter ECU21 is various states of vehicles, such as the vehicle speed, an engine speed value, a switching condition of a door, and a shift range of a gearbox, for displaying on a display, and anti-theft ECU23, It is for supervising a vehicle state and a malicious person invading in vehicles, or sounding a warning sound, when trying to steal each apparatus in vehicles, or calling an external center in emergency dial, and air-conditioner ECU25 is for controlling an air-conditioner.

[0040]In addition, AVC system ECU belonging to the information machines and equipment which perform variety-of-information offers (an information display, reproduction, etc.) of navigation ECU31, audio ECU33, telephone ECU35, and ETC-ECU37 grade is connected to the AVC system network. Navigation ECU31 acquires map data from the map data storage (not shown) which comprises a DVD player connected to self, a CD player, etc.,

and. It is ECU for displaying the map which acquires the information about the current position of vehicles from the GPS receiver (not shown) connected to the communications department 40, and expresses the current position of vehicles based on this on displays (not shown), such as a liquid crystal display connected to audio ECU33 mentioned later, for example.

[0041]Navigation ECU31 acquires congestion information etc. from the VICS walkie-talkie 41 grade mentioned later, It shows a driver to the gate location for ETC by displaying these information on a display with a map, or acquiring the position information on the gate for ETC, etc. from the ETC walkie-talkie 45 mentioned later, and displaying these information on a display.

[0042]Next, according to the instructions as which audio ECU33 was inputted when a user operated the operation switch connected to the ECU concerned, It is for acquiring from the television radio walkie-talkie 43, and reproducing this with the loudspeaker system in vehicles, a liquid crystal display, etc. by controlling the tuner built in the television radio walkie-talkie 43 which mentions later the radio broadcasting program which a user desires, and a television broadcasting program.

[0043]Telephone ECU35 is connected to the external device by which the walkie-talkie 47 for a telephone was connected to the telephone network by communicating between the walkie-talkies 47 for a telephone mentioned later via the base transceiver station in a telephone network, It is for making it communicate through a telephone line between each ECU of mounted LAN10, and an external device.

[0044]In addition, if the order information concerning fee collection, etc. are acquired from an ETC center via an ETC walkie-talkie (after-mentioned), ETC-ECU37, It is because a variety of information is read from the card reader etc. which answered this and were connected to self and this is sent out to an external ETC center via the ETC walkie-talkie 45.

[0045]As the communications department 40 of this example shows drawing 1, then, two or more kinds of walkie-talkies, such as the VICS walkie-talkie 41, the television radio walkie-talkie 43, the ETC walkie-talkie 45, and the walkie-talkie 47 for a telephone, It is ** constituted with the external device terminal area 49 for connecting devices outside a vehicle, such as the service tool 5, into vehicles directly.

[0046]The VICS walkie-talkie 41 comprises a radio wave beacon receiver, a light beacon receiver, etc. for, for example, receiving the road traffic information provided from VICS, and has composition which sends out the commo data from VICS acquired from these walkie-talkies to gateway ECU50.

[0047]The television radio walkie-talkie 43 is provided with the tuner for receiving a television broadcasting signal and a radio broadcast signal, and the tuner is made the composition controlled by the above-mentioned audio ECU33 grade connected to mounted LAN10. This television radio walkie-talkie 43 is made composition connectable with the external center which provides service of a video on demand in response to the instructions

from audio ECU33, and sends out the picture image data etc. which were acquired from these to gateway ECU50.

[0048]The ETC walkie-talkie 45 is a walkie-talkie for communicating between ETC centers, sends out the commo data from an ETC center to gateway ECU50, or transmits the data transmitted from mounted LAN via gateway ECU50 to the ETC center side.

[0049]And the walkie-talkie 47 for a telephone is controlled by the above-mentioned telephone ECU, connects self to an external dial-up line network via a base transceiver station, and sends out the commo data from the dial-up line network to gateway ECU50. Here, the following is mentioned as access from the outside of the car performed via the walkie-talkie 47 for a telephone.

[0050]For example, a vehicle owner inputs the instructions for starting an air-conditioner into the above-mentioned air-conditioner ECU25 in mounted LAN10 from a cellular phone etc., and access in the case of carrying out remote control operation of the air-conditioner is mentioned. Access in case a user acquires composition data through a telephone line and reproduces this in audio ECU33 in vehicles etc. are considered. In addition, a user acquires the program which operates by each ECUs 11-37 in mounted LAN from an external center through a telephone line, this is installed in ECUs 11-37, and access in the case of writing in a program newly or updating it can be considered.

[0051]Although each walkie-talkies 41, 43, 45, and 47 in the communications department 40 were explained above, in the communications system 1 concerned in the car, the case where commo data without directions of a distribution destination (namely, access point) is received from the exterior in the communications department 40 can be considered. Therefore, what is necessary is to give the information about a distribution destination to commo data, and just to constitute the communications department 40, for example about the data of a specific kind without directions of each walkie-talkies 41-47 of a distribution destination, so that this may be transmitted to gateway ECU50 in coping with such a case. For example, when a TV signal is received, it is specifying a distribution destination as audio ECU33 etc.

[0052]In addition, the service tool 5 for the external device terminal area 49 to perform vehicles diagnosis, It comprises a connector for connecting the device outside a vehicle of the service tool 5 grade for updating the program in ECU to mounted LAN10, and if the service tool 5 is connected, it has the composition of connecting the service tool 5 to gateway ECU50.

[0053]It is connected without the communications department 40 and mounted LAN10, and gateway ECU50 has the composition for relaying the data communications between each ECUs 11-37 in mounted LAN10, and the device 3 outside a vehicle. for example, gateway ECU50 has what is called a routing function -- each system in mounted LAN -- access to ECU in the network of the others in mounted LAN from ECU in a network is relayed. If there is a demand of access to ECU in a control system network in a body system network from ECU concretely, the commo data from ECU in a body system network will be transmitted to

ECU in a control system network.

[0054]As a feature which this invention requires, this gateway ECU50 will perform the main routine shown in drawing 2 by own CPU, if the commo data which the communications department 40 received is acquired. The flow chart with which drawing 2 expresses the main routine performed by gateway ECU50, and drawing 3, The flow chart with which called-program transmission processing is expressed by the main routine, and drawing 4 (a) are a flow chart showing the individual authenticating processing called by the program transfer processing, and a flow chart with which drawing 5 expresses access-restriction processing.

[0055]First gateway ECU50 in S110 the distribution destination of commo data, It reads in the commo data and it is judged whether a distribution destination (namely, access point) is what is listed by the in-the-car loading equipment list memorized by the own storage (this example memory) based on this (S120). An in-the-car loading equipment list here is a list about ECUs 11-37 connected to mounted LAN10.

[0056]Here, if it judges that the distribution destination of commo data is not registered into an in-the-car loading equipment list, gateway ECU50 will end the processing concerned, after performing access-restriction processing (in detail after-mentioned) in S125. When it judges that the distribution destination of commo data is registered into the in-the-car loading equipment list, on the other hand, gateway ECU50, In S130 continuing, it is judged whether the commo data is commo data including the information about the write request of the conformity constant for operating exactly the control system in the information about the write request of the program which operates by ECU in mounted LAN10, or vehicles. The write requests of a conformity constant here are things, such as a rewriting demand of an engine ignition-timing map, for example.

[0057]And if it judges that a program or the information about the write request of a parameter is included in commo data, gateway ECU50 will perform program transfer processing (drawing 3) in S140 next. Although only the write request of a program is explained about subsequent processings, these processings are performed in the same procedure, when it is a write request of a conformity constant.

[0058]If it shifts to program transfer processing, gateway ECU50 will demand the device 3 outside a vehicle which has transmitted the write request of the program via the communications department 40 in S141 first to transmit a password to self as the first certification information, and will acquire a password from the device 3 outside a vehicle to it.

[0059]Then, it is judged whether the password of gateway ECU50 corresponds with the password beforehand registered into self (gateway ECU50) in S143. About this password, the producer should just register the password peculiar to that gateway ECU50 into the gateway ECU50 concerned at the time of product shipment, for example.

[0060]And when it judges that a password is not right (it is got blocked and the acquired password and the password registered beforehand are not in agreement) in S143, gateway

ECU50, If the processing concerned is ended and a password judges it as the right in S143 after shifting processing to S169 and performing access-restriction processing (drawing 5), processing will be shifted to S145, a program will be acquired from the device 3 outside a vehicle via the communications department 40, and a temporary storage will be carried out into an own memory.

[0061]Then, gateway ECU50 performs individual authenticating processing (drawing 4) in S150. If it shifts to individual authenticating processing, gateway ECU50 will require reception of a program of ECU (it is hereafter expressed as "write object ECU".) in mounted LAN10 which the device 3 outside a vehicle makes the write object of the program in S151 first.

[0062]Thus, if gateway ECU50 requires reception of a program, write object ECU which received the demand will perform program reception which shows drawing 4 (b) a flow chart. The details of the individual authenticating processing which gateway ECU50 shown in drawing 4 (a) performs hereafter, and the details of the program reception shown in drawing 4 (b) will be explained in parallel.

[0063]Write object ECU which received the request to receipt of the program, In order that the device 3 outside a vehicle which has carried out the write request of a program in S310 first may distinguish whether it is the device 3 outside a vehicle to which the writing of the program was permitted beforehand, the second different certification information from the first certification information of the above is required of the device 3 outside a vehicle of write request origin.

[0064]For example, when common key systems (DES method etc.) are adopted as an authentic method, write object ECU, In S310, generate the random number r and this is once memorized in an own memory, and this random number r is transmitted to the device 3 side outside a vehicle with a demand of certification information, and it directs to return as certification information what enciphered the random number r with the common key K to the device 3 outside a vehicle.

[0065]When requiring this certification information of the device 3 outside a vehicle, once, gateway ECU50 acquires that demand information from write object ECU, and transmits this to the device 3 outside a vehicle via the communications department 40 (S153). Gateway ECU50 will transmit this to write object ECU in S155, if certification information is acquired from the device 3 outside a vehicle as a response result to a demand of this certification information.

[0066]On the other hand, write object ECU will compare this with the certification information memorized in the own memory, if certification information is acquired from the device 3 outside a vehicle via gateway ECU50 (S320) (S330). And if it judged whether attestation of the device 3 outside a vehicle was successful based on the collated result (S340), and attestation was successful, an authentication success will be notified to gateway ECU50 (S350) and attestation will not be successful, what attestation went wrong is notified (S355).

[0067]When the example in the case of attesting the above-mentioned common key system is explained concretely here, write object ECU, Judge whether it is in agreement with the random number r which decoded the certification information acquired from the device 3 outside a vehicle with the common key K and in which this decrypted certification information generated it in S310, and if in agreement, It is reported that attestation of the device 3 outside the vehicle was successful noting that the device 3 outside a vehicle is a device outside a vehicle to which the writing of the program was permitted beforehand (it is Yes at S340).

[0068]On the other hand, gateway ECU50 will judge whether the individual authenticating processing concerned was ended and the attestation by write object ECU was successful in S161 of program transfer processing (drawing 3), if an authentication result (the notice of an authentication success or the notice of an authentication failure) is received from write object ECU in S157.

[0069]That is, if gateway ECU50 will judge it as No by S161, and will move processing to S169, if the notice of an authentication failure is received from write object ECU, and the notice of an authentication success is received from write object ECU, it will judge it as Yes by S161, and will move processing to S163.

[0070]And in S163, gateway ECU50 transmits the program stored temporarily to write object ECU. Corresponding to this, write object ECU receives the program transmitted from gateway ECU50, and memorizes the program in the state which can be performed in an own memory (S360).

[0071]Gateway ECU50 will verify whether write object ECU memorized the program correctly in S165, if write object ECU finishes memorizing a program. For example, gateway ECU50 verifies whether write object ECU memorized the program correctly by comparing whether the program which write object ECU remembered in the memory to be the contents of the program which self transmitted is an identical content.

[0072]And if the program is memorized correctly, out of an own memory. If the program which transmitted in S163 is canceled (S167), the processing concerned is ended and the program is not memorized correctly (it is No at S165), the program again memorized in the own memory is read, and this is transmitted to write object ECU (S163). What is necessary is to stop the writing of a program and just to terminate the processing concerned, when the writing of a program does not work over multiple times.

[0073]Next, processing when gateway ECU50 judges commo data not to be a write request of a program and a conformity constant in S130 (refer to drawing 2) (it is No at S130) is explained. As shown in drawing 2, if gateway ECU50 judges it as No in S130, it will judge whether the distribution destinations (access point) of commo data are AVC system ECUs 31-37 connected to the AVC system network in S170 continuing.

[0074]Here, if it judges that distribution destinations are AVC system ECUs 31-37 (it is Yes at S170), gateway ECU50 will distribute commo data to AVC system ECU of a distribution destination in S175. When a distribution destination judges that they are not AVC system

ECUs 31-37 (it is No at S170), on the other hand, gateway ECU50, Via the communications department 40, the device 3 outside a vehicle which has transmitted the data is required to transmit a password to the addressing to ECU concerned, and the password as certification information is acquired from the device 3 outside a vehicle to it (S180).

[0075]Then, it is judged whether the acquired password is the right by judging whether a password of gateway ECU50 corresponds with the password beforehand registered into self in S190. Gateway ECU50 may be made the composition compared with the same password as having used the password acquired from the device 3 outside a vehicle for comparing by S143 of the program transfer processing mentioned above, and it may be constituted so that it may be another and may compare. In this case, gateway ECU50 is made to memorize both the password beforehand used in the case of collation of S143, and the password used in the case of collation of S190.

[0076]And if it judges that gateway ECU50 transmits data to ECU of a distribution destination (S200), and its a password is not right if a password judges it as the right (it is Yes at S190) (it is No at S190), access-restriction processing will be performed in S195, and the processing concerned will be ended.

[0077]In this access-restriction processing, gateway ECU50 operates, as shown in drawing 5. Namely, it is judged whether gateway ECU50 had access more than n times (for example, 3 times) in the gateway ECU50 concerned within fixed time from the device 3 outside a vehicle same at S410, If n accesses or more cannot be found (it is No at S410), in S420, it will transmit to the walkie-talkies 41-47 with which the communications department 40 corresponds that there was unusual access which failed in attestation from the device 3 outside a vehicle (operation of the walkie-talkies 41-47 corresponding to this is mentioned later), and the processing concerned will be ended.

[0078]On the other hand, when there are n accesses or more, by (S410 Yes), It reports that access from the device 3 outside the vehicle is forbidden to the corresponding walkie-talkies 41-47 (S430), and the walkie-talkies 41-47 are made to keep from sending again the commo data from the device 3 outside a vehicle of the same access origin to gateway ECU50, and the processing concerned is ended to them.

[0079]Each walkie-talkies 41-47 of this example which receive each above-mentioned notice of this access-restriction processing perform access control processing as shown in drawing 6, and control access from the device 3 outside a vehicle. Drawing 6 is a flow chart showing access control processing. It is judged whether when the commo data as a demodulated result is acquired from a demodulator circuit, the walkie-talkies 41-47 acquire the information about the device 3 outside a vehicle of the transmitting origin included in commo data, and identify the transmitting origin (S510), and a transmitting agency is in an access-inhibit list in S520. Whenever this access-inhibit list receives the notice of an access inhibit from gateway ECU50, the walkie-talkies 41-47 update it one by one, and the walkie-talkies 41-47, The access-inhibit list which registered the device 3 outside a vehicle which was the target of the access inhibit into the own memory is held.

[0080]If it judges that transmitting [commo data] origin is in an access-inhibit list in these S520, the walkie-talkies 41-47 will refuse access to gateway ECU50 of the device 3 outside a vehicle of a transmitting agency in S540 continuing. That is, the walkie-talkies 41-47 are canceled, without transmitting the commo data received from the transmitting origin to gateway ECU50.
[0081]On the other hand, if it judges that there is no transmitting [commo data] origin in an access-inhibit list in S520, the walkie-talkies 41-47 will judge whether fixed time lapse is carried out, after the transmitting origin receives unusual access in S530 continuing. Fixed time here is set as time sufficiently shorter than the time at the time of judging whether n accesses or more had gateway ECU50 in S410.
[0082]Here, if it judges that the fixed time after unusual access has not passed, the walkie-talkies 41-47 will move to S540, and will refuse access to gateway ECU50 of the device 3 outside a vehicle of a transmitting agency. If it judges that the fixed time after unusual access has passed, or the notice of unusual access is not received on the other hand, processing will be moved to S550 and commo data will be transmitted to gateway ECU50.
[0083]As mentioned above, although the communications system 1 of this example in the car was explained, The communications department 40 by which gateway ECU50 is connected to the device 3 outside a vehicle in this communications system 1 in the car, When relaying communication between mounted LAN10, the device 3 outside a vehicle if needed Access to each ECUs 11-37 of mounted LAN10. Since it checks by acquiring a password for whether it is the device outside a vehicle to which (namely, data communications with each ECU) were permitted, unjust access to each ECUs 11-37 in mounted LAN10 can be prevented. By having such composition, unjust access can be further prevented from the outside and such a system can consist of cheaply cases where the device 3 outside a vehicle is attested only by individual ECU. In addition, wiring in a communications system in the car can be lessened.
[0084]Commo data programs in the communications system 1 of this example in the car, It is not related with the write request of a conformity constant, and when it is AVC system ECU (ECUs 31-37 connected to the AVC system network) for reporting the information which the distribution destination (access point) of commo data acquired from the exterior to a vehicle occupant, the device 3 outside a vehicle is not attested.
[0085]Though artificiality was made with malicious intent by the commo data as long as it was commo data to AVC system ECUs 31-37, it is because the commo data does not affect the safety about a run of vehicles. It is because the processing load of gateway ECU50 will become high if the device 3 outside a vehicle is attested one by one if it takes that access to AVC system ECU is frequently performed from the outside into consideration. Of course, you may attest individually if necessary at each ECU.
[0086]On the other hand, when the distribution destinations of commo data are ECUs other than AVC system ECU, it is made to attest the device 3 outside a vehicle with a password etc. (when it puts in another way and is ECUs 11-25 connected to the control system

network and the body system network) once at least. It is because each ECU connected to a control system network and a body system network is ECU in connection with vehicle control, so it needs the thing which required these ECUs unjustly and for which it is made not to be shifted and the traveling safety of vehicles is secured.

[0087]Moreover [especially], in the communications system 1 of this example in the car, When commo data is a thing about the write request of a program and a conformity constant, access of the device 3 outside a vehicle is more severely restricted irrespective of the kind of ECU of a distribution destination by performing second attestation in addition to the first attestation with a password etc. Therefore, in the communications system 1 of this example in the car, the situations -- the program which operates in ECU, and the conformity constant concerning vehicle control will be rewritten unjustly -- can be prevented.

[0088]In addition, in this communications system 1 in the car, Since access from the device 3 outside a vehicle with attestation going wrong [much] is forbidden with n authentication failures and he is trying not to input the commo data from the device 3 outside a vehicle into gateway ECU50 in the communications department 40, The problem of the processing load of gateway ECU50 increasing by unlawful access is solvable.

[0089]Here, the relation of the communications system 1 of this example in the car and the communications system of this invention in the car which were explained above is as follows. First, the repeating installation for vehicles of this invention is equivalent to gateway ECU50 of this example, and the information system device of this invention, It is equivalent to AVC system ECUs 31-37 connected to the above-mentioned AVC system network, and the control system equipment of this invention is equivalent to each ECUs 11-25 connected to the above-mentioned control system network or the body system network. The access request of the device outside a vehicle is equivalent to the operation in which the device 3 outside a vehicle transmits commo data to the communications department 40.

[0090]And based on the distribution destination where gateway ECU50 has grasped the first identification device of this invention by S110, It is equivalent to the operation which judges whether a distribution destination is AVC system ECU as an information system device in S170, and the first authentication means is equivalent to the operation whose gateway ECU50 acquires the password as the first certification information in S180, and judges whether a password is the right in S190. The first distribution means is equivalent to processing of S200 performed when it is judged as Yes by S175 and S190 which are performed when gateway ECU50 judges it as Yes by S170.

[0091]In addition, the second identification device of this invention is equivalent to the processing operation of S130 to perform, and gateway ECU50 the second authentication means, When gateway ECU50 judges an access request not to be write requests, such as a program, while shifting a step to S170, when access requests are write requests, such as a program, it is equivalent to the operation which performs processing of S140-S161. Gateway ECU50 shifts a step to S163 based on the decision result of S161, and the second distribution means is equivalent to the operation which transmits commo data

(program etc.) to ECU.

[0092]As mentioned above, although the example of this invention was described, the repeating installation for vehicles and the communications system in the car of this invention are not limited to the above-mentioned example, and can take various modes. For example, although it had composition which attests the device 3 outside a vehicle with a password first in the above-mentioned example, the device 3 outside a vehicle may be attested with other authentication methods. If the device 3 outside a vehicle is attested with an authentication method more reliable than those, such as a common key system, authentication time may become long, but unlawful access to ECU in mounted LAN10 can be prevented more certainly.

[0093]In addition, when write requests, such as a program, were received, are a different authentication method, and had composition which attests the device 3 outside a vehicle twice, but. In order to secure the safety about these writing, it may attest 3 times or more with a reliable authentication method, and the system concerned may be built only once so that the device 3 outside a vehicle may be attested with a very reliable authentication method.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the composition of the communications system 1 of this example in the car.
[Drawing 2]It is a flow chart showing the main routine which gateway ECU50 performs.
[Drawing 3]It is a flow chart showing the program transfer processing which gateway ECU50 performs.
[Drawing 4]They are a flow chart (a) showing the individual authenticating processing which gateway ECU50 performs, and a flow chart (b) showing the program reception which write object ECU performs.
[Drawing 5]It is a flow chart showing the access-restriction processing which gateway ECU50 performs.
[Drawing 6]It is a flow chart showing the access control processing which each walkie-talkies 41-47 perform.
[Description of Notations]
1 [-- ECU, 40 / -- The communications department, 41, 43, 45, 47 / -- A walkie-talkie, 49 / -- An external device terminal area, 50 / -- Gateway ECU] -- A communications system in the car, 3 -- The device outside a vehicle, 10 -- Mounted LAN, 11-37

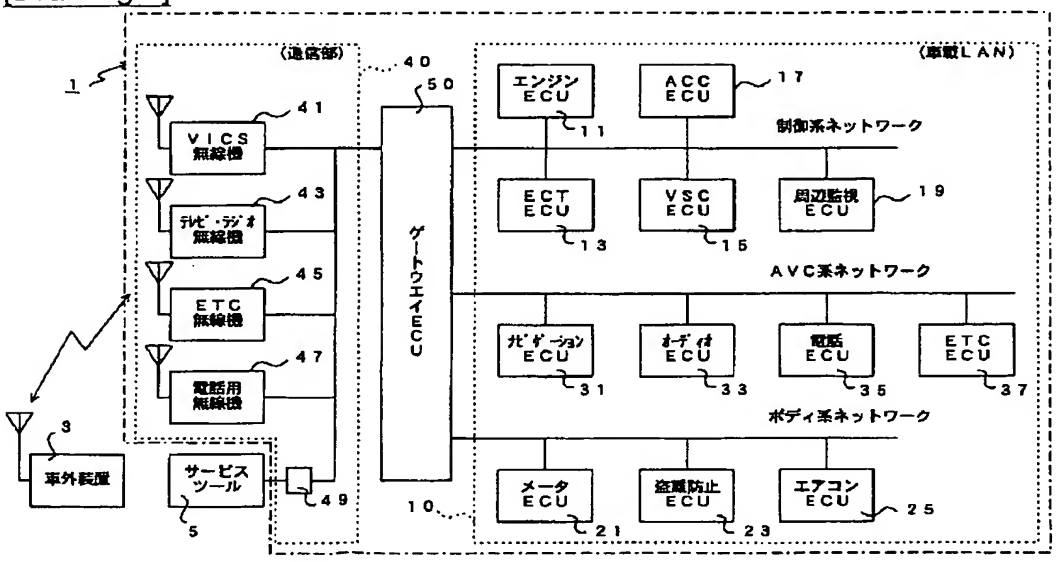
[Translation done.]

* NOTICES *

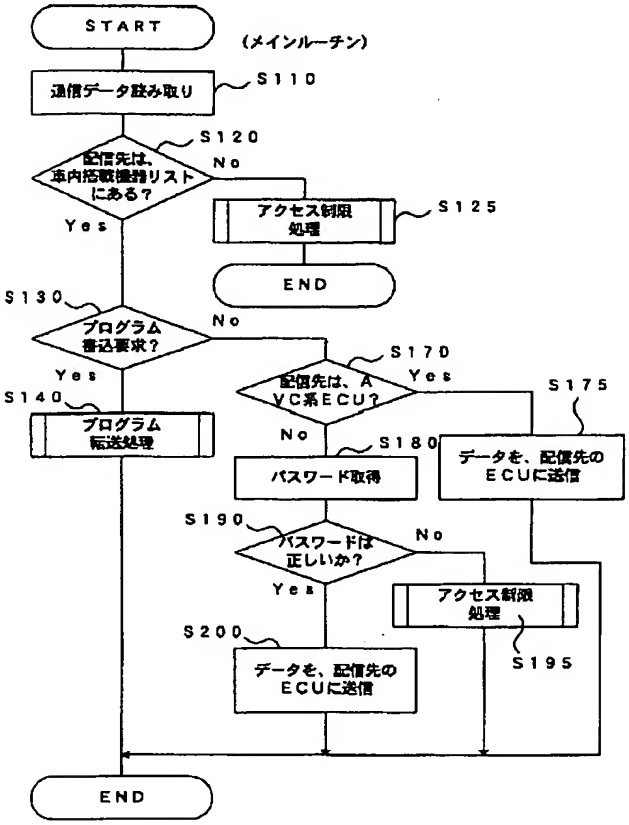
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

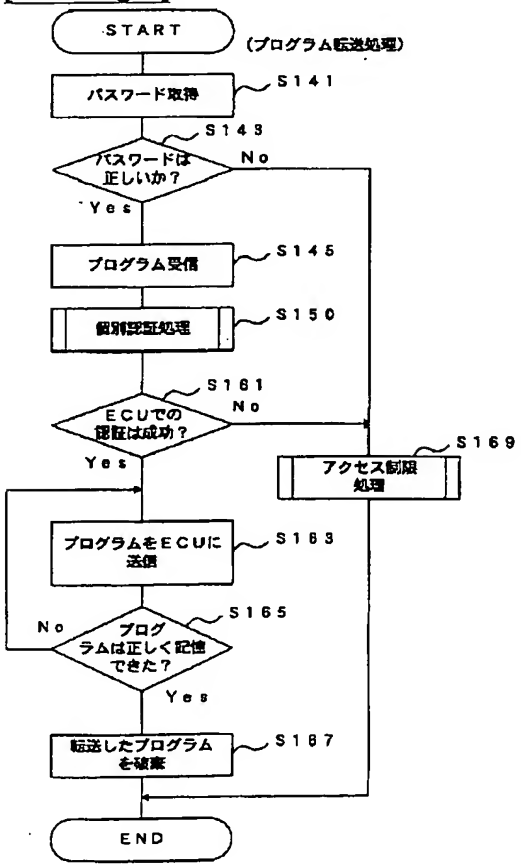
[Drawing 1]



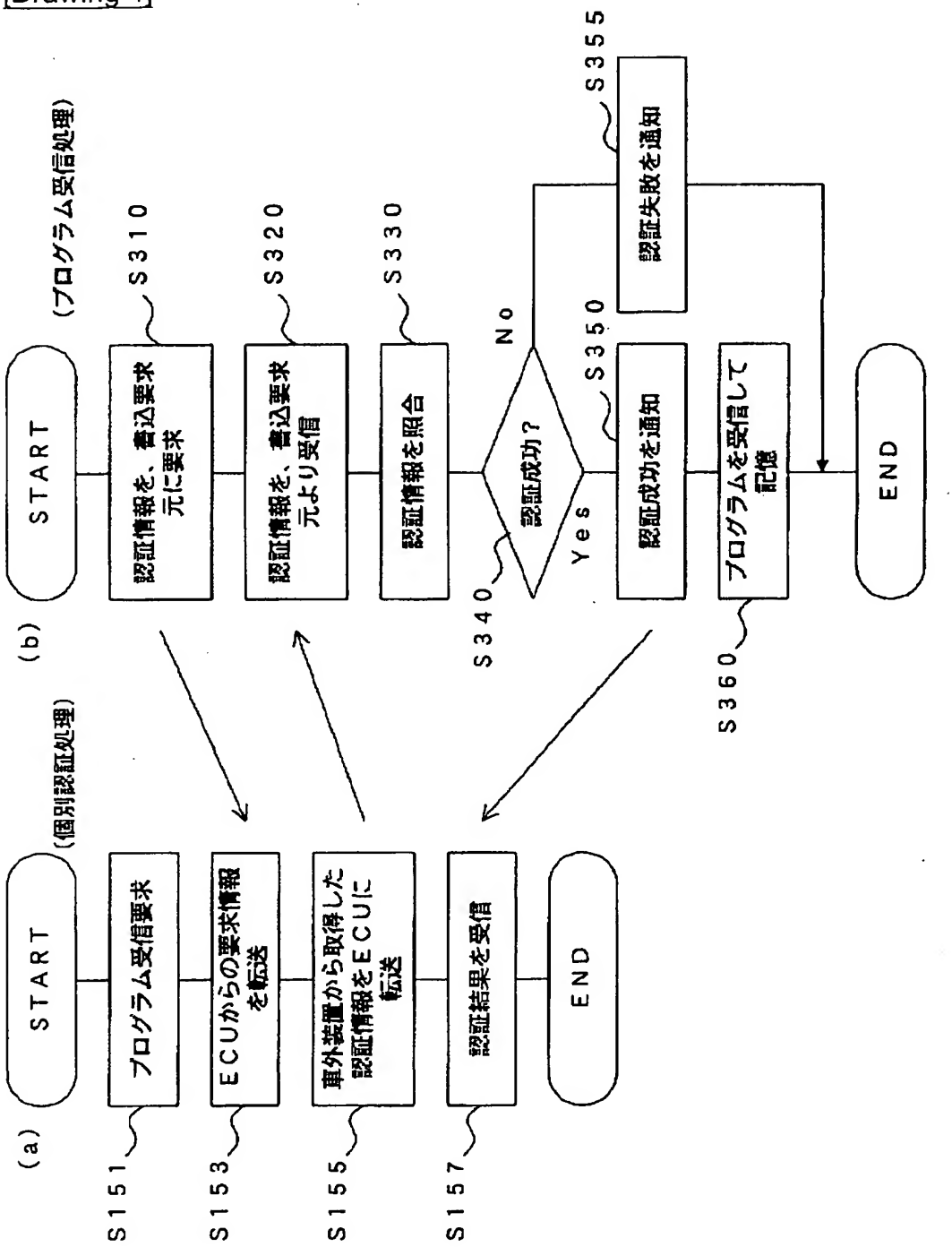
[Drawing 2]


START
(メインルーチン)
通信データ読み取り
S110
配信先は、車内搭載機器リストにある？
S120
No
Yes
アクセス制限処理
S125
END
S130
プログラム書込要求？
No
Yes
S140
プログラム転送処理
S170
配信先は、AVC系ECU？
Yes
S175
No
S180
パスワード取得
データを、配信先のECUに送信
S190
パスワードは正しいか？
No
Yes
アクセス制限処理
S200
S195
データを、配信先のECUに送信
END

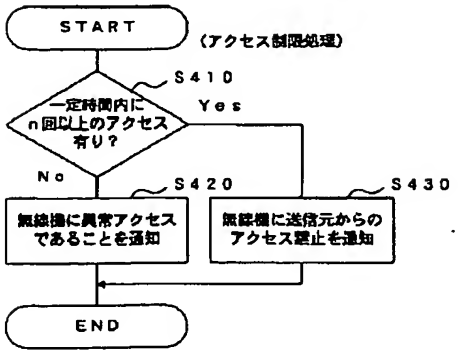
[Drawing 3]


START
(プログラム転送処理)
パスワード取得
S141
S143
パスワードは正しいか？
No
Yes
プログラム受信
S145
個別認証処理
S150
S161
ECUでの認証は成功？
No
Yes
S169
アクセス制限処理
プログラムをECUに送信
S163
S165
No
プログラムは正しく記憶できた？
Yes
転送したプログラムを破棄
S167
END

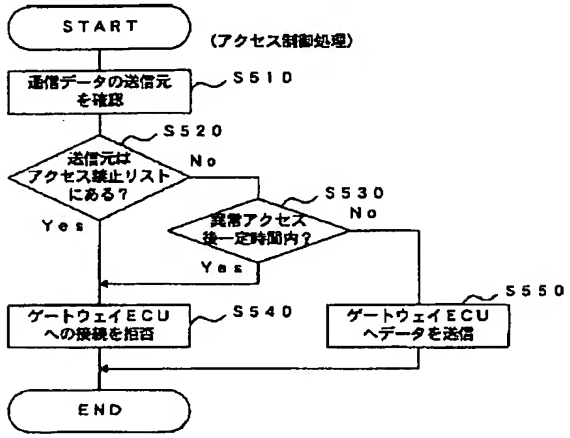
[Drawing 4]



[Drawing 5]



[Drawing 6]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－46536
（Ｐ2003－46536Ａ）
(43)公開日　平成15年２月14日(2003.2.14)

(51)Int.Cl.'		識別記号	Ｆ Ｉ		テーマコード'(参考)
Ｈ０４Ｌ	12/46	１００	Ｈ０４Ｌ 12/46	１００Ｃ	５Ｋ０３２
	12/28	１００	12/28	１００Ａ	５Ｋ０３３
		３１０		３１０	
	12/40		12/40	Ｚ	

審査請求　未請求　請求項の数６　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－231673(Ｐ2001－231673)

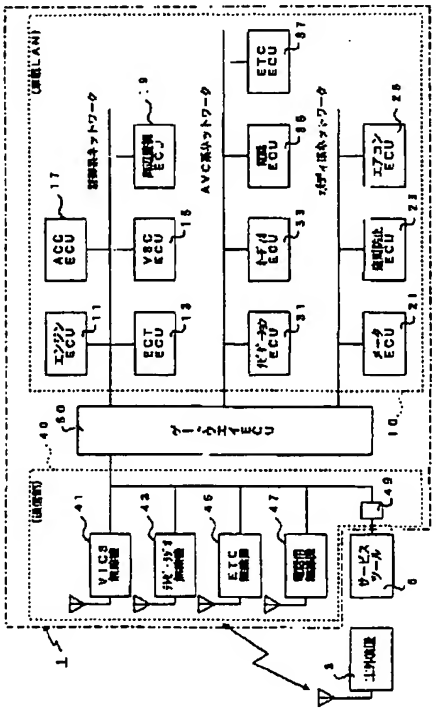
(22)出願日　平成13年７月31日(2001.7.31)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町１丁目１番地
(72)発明者　秋山　進
愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
(74)代理人　100082500
弁理士　足立　勉

Ｆターム(参考)　5K032 AA08 BA06 DA21 DB26
5K033 AA08 BA06 DB18

(54)【発明の名称】　車両用中継装置、及び、車内通信システム

(57)【要約】
【課題】　車内通信システムにおける配線を簡素化しつつ、各種車両内電子装置に対する外部からの不正アクセスを十分に防止する。
【解決手段】　車内通信システム１は、車両内の各ＥＣＵ１１～３７が接続された車載ＬＡＮ１０と、車外装置３との間で通信を行うための通信部４０と、車載ＬＡＮと通信部との間に配置され車載ＬＡＮ内の各ＥＣＵと車外装置とのデータ通信を中継するゲートウェイＥＣＵ５０と、から構成されている。ゲートウェイＥＣＵは、車外装置から通信部を介して車載ＬＡＮ内のＥＣＵに対するプログラムの書込要求があると、自身で車外装置を認証すると共に、プログラムの書込対象のＥＣＵに、車外装置を認証させる。また、ゲートウェイＥＣＵは、プログラム等の書込要求以外の通信データを受信した場合に、それがＡＶＣ系ネットワーク内のＥＣＵ３１～３７を配信先とするものでないと判断すると自身で車外装置の認証を行う。



【特許請求の範囲】
【請求項１】　車両に構築された車載ＬＡＮと、車外装置との間でデータ通信を行う通信装置との間に配置され、該通信装置を介して接続される車外装置と車載ＬＡＮに接続された各種車両内電子装置との間の通信を中継する車両用中継装置であって、
車外装置から前記車載ＬＡＮ内の車両内電子装置へのアクセス要求があると、そのアクセス先を識別すると共に、該識別結果に基づいて、該アクセス要求が車外装置の認証を必要とする前記車両内電子装置へのアクセス要求であるか否かを判断する第一識別手段と、
前記第一識別手段が、前記アクセス要求を前記車外装置の認証を必要とするものであると判断すると、前記車外装置から送信されてきた第一の認証情報に基づき、前記車外装置が予め前記車両内電子装置へのアクセスを許可された車外装置であるか否かを判断する第一認証手段と、
該第一認証手段が、前記アクセス要求してきた車外装置を予め前記車両内電子装置へのアクセスを許可された車外装置であると判断するか、前記第一識別手段が、前記アクセス要求を前記車外装置の認証を必要としないものであると判断すると、前記車外装置から前記通信装置を介して送信されてきた通信データを、アクセス先の前記車両内電子装置に配信する第一配信手段と、
を備えたことを特徴とする車両用中継装置。
【請求項２】　前記車載ＬＡＮには、前記車両内電子装置として、外部より取得した情報を車両乗員に報知するための情報系装置と、車両を制御するための制御系装置と、が接続されており、
前記第一識別手段は、前記車両内電子装置へのアクセス要求があると、該アクセス要求が、前記情報系装置及び前記制御系装置のいずれのアクセス要求であるかを識別することにより、該アクセス要求が、前記車外装置の認証を必要とする前記車両内電子装置へのアクセス要求であるか否かを判断し、
前記第一認証手段は、前記第一識別手段が前記アクセス要求を前記制御系装置へのアクセス要求であると判断すると、前記車外装置から送信されてきた第一の認証情報に基づき、前記車外装置が、予め前記車両内電子装置へのアクセスを許可された車外装置であるか否かを判断することを特徴とする請求項１に記載の車両用中継装置。
【請求項３】　前記車外装置から前記車両内電子装置へのアクセス要求があると、該アクセス要求が、車両内電子装置にて動作するプログラム又は車両内電子装置動作用のパラメータを書き込むための書込要求であるか否かを判断する第二識別手段と、
前記第二識別手段が、前記車両内電子装置へのアクセス要求を前記書込要求ではないと判断すると、前記第一識別手段を動作させ、前記第二識別手段が、前記車両内電子装置へのアクセス要求を前記書込要求であると判断すると、前記車外装置から送信されてきた第二の認証情報に基づき、前記書込要求してきた車外装置が、前記車両内電子装置にて動作するプログラム又は前記車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断する第二認証手段と、
該第二認証手段が、前記書込要求してきた車外装置を前記車両内電子装置にて動作するプログラム又は前記車両内電子装置動作用のパラメータの書込を許可された車外装置であると判断した場合にのみ、該車外装置から前記通信装置を介して送信されてきた通信データを、アクセス先の前記車両内電子装置に配信する第二配信手段と、
を備えたことを特徴とする請求項１又は請求項２に記載の車両用中継装置。
【請求項４】　前記第二認証手段は、前記第二識別手段が前記車両内電子装置へのアクセス要求を前記書込要求であると判断すると、前記第一の認証情報に基づき前記車外装置が予め前記車両内電子装置へのアクセスを許可された車外装置であるか否かを判断し、前記車外装置が予め前記車両内電子装置へのアクセスを許可された車外装置であると、前記第二の認証情報に基づき、前記書込要求してきた車外装置が、前記車両内電子装置にて動作するプログラム又は前記車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断することを特徴とする請求項３に記載の車両用中継装置。
【請求項５】　前記第二認証手段は、前記車外装置から送信されてきた前記第一の認証情報を、自身が所有する認証情報と照合することにより、前記車外装置が予め前記車両内電子装置へのアクセスを許可された車外装置であるか否かを判断し、前記車外装置が予め前記車両内電子装置へのアクセスを許可された車外装置であると、前記車外装置から送信されてきた前記第二の認証情報を、前記プログラム又は前記パラメータの書込対象となる前記車両内電子装置に転送して、該車両内電子装置に前記第二の認証情報を該車両内電子装置が所有する認証情報と照合させると共に、該照合結果を該車両内電子装置から取得し、該取得した照合結果に基づいて、前記書込要求してきた車外装置が、前記車両内電子装置にて動作するプログラム又は前記車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断することを特徴とする請求項４に記載の車両用中継装置。
【請求項６】　車両に構築された車載ＬＡＮと、
車外装置との間でデータ通信を行う通信装置と、
該通信装置と、前記車載ＬＡＮとの間に配置され、前記通信装置を介して接続される車外装置と前記車載ＬＡＮに接続された各種車両内電子装置との間の通信を中継する請求項１～請求項５のいずれかに記載の車両用中継装置と、
を備えたことを特徴とする車内通信システム。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】本発明は、通信装置を介して接続される車外装置と、車載ＬＡＮに接続された各種車両内電子装置との間の通信を中継する車両用中継装置に関する。

【０００２】

【従来の技術】近年の車両、特に自動車においては、制御装置、情報機器、オーディオ機器、といった各種車両内電子装置の搭載数が増加傾向にあり、装置相互間での連携動作若しくは情報の共有化が必要な車両内電子装置については、各装置相互間で情報を送受信できるように、専用の通信線で接続し、情報通信用ネットワーク（所謂、車載ＬＡＮ）を構築するのが一般的である。

【０００３】また、近年においては車両外のネットワークが発達したことに伴い、車両内の各装置に必要な各種情報を車両外から取得できるようなインフラが整備され、これに伴い、車外装置との間で通信を行うための無線機を備えた車両内電子装置を、数多く車載ＬＡＮに接続する例が増えてきている。

【０００４】例えば、道路交通情報通信システム（ＶＩＣＳ）から提供される道路交通情報を受信可能なＶＩＣＳ無線機や外部のインターネットから近辺の店舗情報を収集するなどの目的で使用する携帯電話等を接続可能なナビゲーション装置、自動料金課金システム（ＥＴＣ）との間で通信を行うためのＥＴＣ無線機が接続されたＥＴＣ車載器等である。

【０００５】

【発明が解決しようとする課題】しかしながら、従来の車載ＬＡＮにおいては、外部から各種情報を取得するための無線機を、その情報を主に使用する機器に直接接続するような構成となっていたため、その無線機が車内の所望の位置に配置できなかったり、無線機と機器との間の余分な配線をしなければならず不便であった。

【０００６】この問題点を解消するためには、例えば、車載ＬＡＮに無線機を直接接続して、無線機が受信した情報を必要とする車載ＬＡＮ内の装置が、その車載ＬＡＮを介して、無線機から必要な情報を取得できるようにする方法が考えられる。このようにすれば、無線機等の設置位置の自由度が高く、更には配線数も少なく済み便利である。

【０００７】しかし、このような構成であると、無線機を介して、車両外から車載ＬＡＮに接続された各装置にアクセスすることが可能となり、近年インターネット等の分野で、多発するネットワーク端末への不正アクセスと同様の問題が発生する可能性が高い。

【０００８】本発明は、こうした問題に鑑みなされたものであり、車内通信システムにおける配線を簡素化しつつ、車両内の各種車両内電子装置に対する外部からの不正アクセスを十分に防止することを目的とする。

【０００９】

【課題を解決するための手段】かかる目的を達成するためになされた請求項１に記載の発明においては、車両に構築された車載ＬＡＮと、車外装置との間でデータ通信を行う通信装置との間に配置され、その通信装置を介して接続される車外装置と車載ＬＡＮに接続された各種車両内電子装置との間の通信を中継する車両用中継装置に、第一識別手段と、第一認証手段と、第一配信手段と、が備えられている。

【００１０】即ち、本発明の車両用中継装置は、車外装置から車載ＬＡＮに接続された車両内電子装置へのアクセス要求があると、第一識別手段にて、そのアクセス先を識別すると共に、その識別結果に基づいて、アクセス要求が車外装置の認証を必要とする車両内電子装置へのアクセス要求であるか否かを判断する。

【００１１】また、車両用中継装置は、第一識別手段がそのアクセス要求を車外装置の認証を必要とするものであると判断すると、第一認証手段にて、車外装置から送信されてきた第一の認証情報に基づき、車外装置が予め車両内電子装置へのアクセスを許可された車外装置であるか否かを判断する。

【００１２】更に、車両用中継装置は、第一認証手段がアクセス要求してきた車外装置を予め車両内電子装置へのアクセスを許可された車外装置であると判断した場合、もしくは、第一識別手段がアクセス要求を車外装置の認証を必要としないものであると判断した場合に、第一配信手段にて、車外装置から通信装置を介して送信されてきた通信データを、アクセス先の車両内電子装置に配信する。

【００１３】したがって、請求項１に記載の車両用中継装置は、車載ＬＡＮに車外装置を接続する前に、車載ＬＡＮ内の車両内電子装置へのアクセスが許可されていない車外装置からのアクセスに関して、その車両内電子装置へのアクセスを拒否することができる。換言すると、車両用中継装置は、第一認証手段で車外装置の認証を行うことにより外部からのアクセスを制限することができ、結果、外部の不正アクセスを防止することができる。

【００１４】尚、第一識別手段に、アクセス要求が車外装置の認証を必要とする車両内電子装置へのアクセス要求であるか否かを判断させる方法としては、例えば、予め車両用中継装置内に、車外装置の認証を必要とする車両内電子装置をリストアップしておき、第一識別手段に、そのリストに基づき車外装置の認証を必要とするか否か判断させる方法がある。この他、車載ＬＡＮとして、車両内電子装置の系統別に複数の独立したネットワークを構築して、これらのネットワークには車両用中継装置を介さなければ外部からアクセスできないようにしておき、第一識別手段に、アクセス要求がどの系統のネットワークに属する車両内電子装置へのアクセス要求か否か判断させることにより、アクセス要求が車外装置の認証を必要とするものか否か判断させてもよい。

【００１５】また、この際に車外装置の認証が必要となった場合の認証方法としては、例えば、予め車両内電子装置毎の認証情報（パスワード等）を車両用中継装置に記憶させておき、車両用中継装置に、その認証情報と車外装置から取得した認証情報とを照合させる方法がある。また別の例として、車両用中継装置に車両内電子装置共通の認証情報を記憶させておき、車外装置の認証が必要なアクセス要求があった場合には、アクセス先に関係なく、共通の認証情報にて車外装置の認証を行わせてもよい。

【００１６】この他、車載ＬＡＮに接続されている車両内電子装置を、外部より取得した情報を車両乗員に報知するための情報系装置と、車両を制御するための制御系装置とに区分して、第一識別手段に、アクセス要求が、情報系装置及び制御系装置の内どちらのアクセス要求であるかを識別させることにより、車外装置の認証が必要か否か判断させてもよい。

【００１７】また、この場合においては、請求項２に記載のように、第一識別手段がアクセス要求を制御系装置へのアクセス要求であると判断した場合に、第一認識手段が車外装置の認証を上記方法にて行うように車両用中継装置を構成しておくのがよい。

【００１８】このようにしておけば、車両を制御するための制御系装置には、認証を受けた正当な車外装置からしかアクセスできないことになり、車両用中継装置は、車両の走行に係わる制御系装置への不正アクセスを防止することができる。ところで、以上においては、アクセス先を識別することにより車外装置の認証が必要か否かを判断する手法をとったが、車外装置からのアクセス要求の種類（通信データの種類等）によっては、アクセス先にかかわらず車外装置を認証したほうが良い場合も考えられる。

【００１９】例えば、アクセス要求が、車両内電子装置にて動作するプログラムや、車両内電子装置動作用のパラメータ（例えば、車両内の制御システムを的確に動作させるための適合定数）を書き込むための書込要求である場合などである。このため、請求項３に記載の車両用中継装置においては、第一識別手段、第一認証手段、第一配信手段に加えて、第二識別手段と、第二認証手段と、第二配信手段と、を設けている。

【００２０】即ち、請求項３に記載の車両用中継装置は、車外装置から車両内電子装置へのアクセス要求があると、第二識別手段にて、そのアクセス要求が、車両内電子装置にて動作するプログラム又は車両内電子装置動作用のパラメータを書き込むための書込要求であるか否かを判断し、第二識別手段が車両内電子装置へのアクセス要求を書込要求ではないと判断すると、第二認証手段が第一識別手段を動作させる構成にされている。

【００２１】また、この車両用中継装置は、第二識別手段が、車両内電子装置へのアクセス要求をプログラム又は車両内電子装置動作用のパラメータの書込要求であると判断すると、車外装置から送信されてきた第二の認証情報に基づき、第二認証手段にて、書込要求してきた車外装置が車両内電子装置にて動作するプログラム又は車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断する。

【００２２】そして、その第二認証手段が書込要求してきた車外装置を車両内電子装置にて動作するプログラム又は車両内電子装置動作用のパラメータの書込を許可された車外装置であると判断した場合にのみ、第二配信手段にて、車外装置から通信装置を介して送信されてきた通信データとしてのプログラム又は車両内電子装置動作用のパラメータを、アクセス先の車両内電子装置に配信する。

【００２３】したがって、請求項３に記載の車両用中継装置においては、アクセス要求がプログラム又は車両内電子装置動作用のパラメータの書込要求であった場合に、アクセス先に関係なく、第二の認証情報に基づいて、車外装置を認証することができ、結果、不正なアクセスによる車両内電子装置へのプログラム、車両内電子装置動作用のパラメータの書込を防止することができる。

【００２４】勿論、正当な車外装置からの書込要求であった場合には、第二配信手段にて、プログラム又は車両内電子装置動作用のパラメータがアクセス先の車両内電子装置に配信されるしくみになっているため、当該車両用中継装置によれば、不正アクセスによるプログラム及び車両内電子装置動作用のパラメータの書込を防止しつつ、正当なユーザには、簡単に車両内電子装置のプログラム、車両内電子装置動作用のパラメータを書込・更新させることができる。

【００２５】例えば、従来では、ディーラ等が専用の機器で車両内電子装置のプログラムを更新させていたが、このような車両用中継装置が組み込まれた車両内においては、ディーラに車両を持ち込むような煩わしい事を運転者等に強いることなく、プログラムを更新することができる。

【００２６】尚、請求項３に記載の車両用中継装置においては、アクセス要求がプログラム又は車両内電子装置動作用のパラメータの書込であった場合の認証方式を、より確実に車外装置が正当なものであるかを判断できるような強固な認証方式にしておくのが望ましい。

【００２７】このためには、例えば、請求項４に記載のように、第二識別手段が車両内電子装置へのアクセス要求を書込要求であると判断すると、第二認証手段が、第一の認証情報に基づき車外装置が予め車両内電子装置へのアクセスを許可された車外装置であるか否かを判断し、車外装置が予め車両内電子装置へのアクセスを許可された車外装置であると、第二の認証情報に基づき、書込要求してきた車外装置が、車両内電子装置にて動作す

るプログラム又は車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断するように車両用中継装置を構成するのがよい。

【００２８】このように車両用中継装置を構成すれば、第一の認証情報及び第二の認証情報に基づき、二段階で車外装置を認証することができるので、より確実にプログラム、車両内電子装置動作用のパラメータの書込要求が、正当な車外装置からのものであるかを判別することができる。したがって、本発明の車両用中継装置（請求項４）によれば、車載ＬＡＮに接続された車両内電子装置への不正アクセスをより確実に防止することができる。

【００２９】尚、具体的には、請求項４に記載の車両用中継装置を請求項５に記載のように構成するのが好ましい。請求項５に記載の車両用中継装置では、第二認証手段が、車外装置を認証するための認証情報を所有しており、車外装置から送信されてきた第一の認証情報を、自身が所有するその認証情報と照合することにより、車外装置が予め車両内電子装置へのアクセスを許可された車外装置であるか否かを判断するように構成されている。

【００３０】また、この第二認証手段は、車外装置が予め車両内電子装置へのアクセスを許可された車外装置であると判断すると、車外装置から送信されてきた第二の認証情報を、プログラム又は車両内電子装置動作用のパラメータの書込対象となる車両内電子装置に転送する。

【００３１】尚、この転送された第二の認証情報を受け取る車両内電子装置には、車外装置がプログラム又は車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断するための認証情報が記憶されており、第二認証手段は、第二の認証情報を転送することにより、車両内電子装置に、第二の認証情報をその車両内電子装置が所有する認証情報と照合させる。また、その照合結果を車両内電子装置から取得し、取得した照合結果に基づいて、書込要求してきた車外装置が、車両内電子装置にて動作するプログラム又は車両内電子装置動作用のパラメータの書込を許可された車外装置であるか否かを判断する。

【００３２】このような認証方法で車外装置を認証する請求項５に記載の車両用中継装置では、第二の認証を、そのプログラム又はパラメータの書込対象の車両内電子装置に行わせるため、車両用中継装置が万が一不正アクセスにより誤動作した場合においても、不正なプログラム、車両内電子装置動作用のパラメータの書込を防止することができる。また、車載ＬＡＮに直接装置を接続し、車両内電子装置に不正アクセスしようとする行為に対しても、それを防止することができる。

【００３３】また、以上に説明した請求項１～請求項５のいずれかに記載の車両用中継装置を用いれば、不正アクセスに耐える車内通信システムを構築することができる。尚具体的には、請求項６に記載のように、請求項１～請求項５のいずれかに記載の車両用中継装置を、車外装置との間でデータ通信を行う通信装置と、車両に構築された車載ＬＡＮとの間に配置して、その車両用中継装置に、通信装置を介して接続される車外装置と車載ＬＡＮに接続された各種車両内電子装置との間の通信を中継させればよい。

【００３４】この際、車両内に搭載される全ての通信装置を、車両用中継装置に接続すれば、車外装置からのアクセスを、全て車両用中継装置で中継することができて、不正アクセスを、全て車両用中継装置で対処させることができる。したがって、そのような車内通信システムにおいては、車両内電子装置への不正アクセスをより確実に防止することができる。

【００３５】

【発明の実施の形態】以下に本発明の実施例について、図面とともに説明する。図１は、本発明が適用された車内通信システム１の構成を表すブロック図である。

【００３６】図１に示すように、本実施例の車内通信システム１は、車両内電子装置として車両内に設置された各電子制御装置（ＥＣＵ１１～３７）により構築された車載ＬＡＮ１０と、車外装置３との間で通信を行うための通信部４０と、車載ＬＡＮ１０と、通信部４０との間に配置され、車載ＬＡＮ１０内の各ＥＣＵ１１～３７と車外装置３との間のデータ通信を中継するゲートウェイＥＣＵ５０と、から構成されている。

【００３７】車両内に構築された上記車載ＬＡＮ１０は、制御系ネットワークと、ＡＶＣ系ネットワークと、ボディ系ネットワークと、からなり、夫々のネットワークには、共通の伝送線に、各系統に対応する車両内の上記ＥＣＵが接続されている。例えば、制御系ネットワークには、エンジンＥＣＵ１１、ＥＣＴ・ＥＣＵ１３、ＶＳＣ・ＥＣＵ１５、ＡＣＣ・ＥＣＵ１７、周辺監視ＥＣＵ１９等の走行に係わる車両制御用のＥＣＵが接続されている。

【００３８】ここで、エンジンＥＣＵ１１は、エンジンを制御するエンジン制御装置であり、ＥＣＴ・ＥＣＵ１３は、自動変速機の変速制御を行う変速制御装置であり、これらは所謂パワートレイン系の制御装置である。また、ＶＳＣ・ＥＣＵ１５は、車両の姿勢制御及び制動制御を行う制御装置であり、ＡＣＣ・ＥＣＵ１７は、車両を先行車両に追従させる制御を行う走行制御装置であり、これらは、所謂車両運動系の制御装置である。

【００３９】一方、ボディ系ネットワークには、メータＥＣＵ２１、盗難防止ＥＣＵ２３、エアコンＥＣＵ２５等のボディ制御用のＥＣＵが接続されている。メータＥＣＵ２１は、車速、エンジン回転数、ドアの開閉状態、変速機のシフトレンジ等、車両の各種状態を表示装置に表示するためのものであり、盗難防止ＥＣＵ２３は、車両状態を監視して、悪意の者が車両内に侵入したり車両内の各機器を盗もうとしている場合に、警報音を鳴らし

たり、外部センタに緊急通報をするためのものであり、エアコンＥＣＵ２５は、エアコンを制御するためのものである。

【００４０】この他、ＡＶＣ系ネットワークには、ナビゲーションＥＣＵ３１、オーディオＥＣＵ３３、電話ＥＣＵ３５、ＥＴＣ・ＥＣＵ３７等の各種情報提供（情報表示、再生等）を行う情報機器に属するＡＶＣ系ＥＣＵが接続されている。ナビゲーションＥＣＵ３１は、自身に接続されたＤＶＤプレーヤやＣＤプレーヤ等から構成される地図データ格納部（図示せず）から地図データを取得すると共に、通信部４０に接続されたＧＰＳ受信機（図示せず）から車両の現在位置に関する情報を取得し、これに基づいて車両の現在位置を表す地図を、例えば、後述するオーディオＥＣＵ３３に接続された液晶ディスプレイ等の表示装置（図示せず）に表示するためのＥＣＵである。

【００４１】また、ナビゲーションＥＣＵ３１は、後述するＶＩＣＳ無線機４１等から、渋滞情報等を取得して、これらの情報を地図と共に表示装置に表示したり、後述するＥＴＣ無線機４５から、ＥＴＣ用のゲートの位置情報等を取得して、これらの情報を表示装置に表示することにより、運転者にＥＴＣ用のゲート位置を案内する。

【００４２】次に、オーディオＥＣＵ３３は、利用者が当該ＥＣＵに接続された操作スイッチを操作することにより入力された指令に従って、利用者が望むラジオ放送番組やテレビ放送番組を、後述するテレビ・ラジオ無線機４３に内蔵されたチューナーを制御することによりテレビ・ラジオ無線機４３から取得して、これを車両内のスピーカシステムや、液晶ディスプレイ等にて再生するためのものである。

【００４３】また、電話ＥＣＵ３５は、後述する電話用無線機４７との間で通信を行うことにより電話用無線機４７を電話回線網に接続された外部装置に電話回線網内の無線基地局を介して接続して、車載ＬＡＮ１０の各ＥＣＵと外部装置との間で電話回線を通じて通信を行わせるためのものである。

【００４４】この他、ＥＴＣ・ＥＣＵ３７は、課金に係る指令情報等を、ＥＴＣセンタからＥＴＣ無線機（後述）を介して取得すると、これに応答して自身に接続されたカードリーダ等から各種情報を読み出し、これをＥＴＣ無線機４５を介して外部のＥＴＣセンタに送出するためのものである。

【００４５】続いて、本実施例の通信部４０は、図１に示すように、ＶＩＣＳ無線機４１、テレビ・ラジオ無線機４３、ＥＴＣ無線機４５、電話用無線機４７などの複数種類の無線機と、サービスツール５などの車外装置を直接車両内に接続するための外部装置接続部４９と、から構成されている。

【００４６】ＶＩＣＳ無線機４１は、例えば、ＶＩＣＳから提供される道路交通情報を受信するための電波ビーコン受信機や、光ビーコン受信機などから構成されており、これらの無線機から取得したＶＩＣＳからの通信データをゲートウェイＥＣＵ５０に送出する構成となっている。

【００４７】テレビ・ラジオ無線機４３は、テレビ放送信号や、ラジオ放送信号を受信するためのチューナを備え、そのチューナは、車載ＬＡＮ１０に接続された上記オーディオＥＣＵ３３等に制御される構成にされている。また、このテレビ・ラジオ無線機４３は、オーディオＥＣＵ３３からの指令を受けて、ビデオオンデマンドのサービスを提供する外部センタに接続可能な構成にされており、これらから取得した映像データ等をゲートウェイＥＣＵ５０に送出する。

【００４８】また、ＥＴＣ無線機４５は、ＥＴＣセンタとの間で通信を行うための無線機であり、ＥＴＣセンタからの通信データをゲートウェイＥＣＵ５０に送出したり、ゲートウェイＥＣＵ５０を介して車載ＬＡＮから送信されてきたデータをＥＴＣセンタ側に送信する。

【００４９】そして、電話用無線機４７は、上記電話ＥＣＵに制御されて、自身を無線基地局を介して外部の公衆電話回線網に接続し、その公衆電話回線網からの通信データをゲートウェイＥＣＵ５０に送出する。ここで、電話用無線機４７を介して行われる車外からのアクセスとしては、以下のようなものが挙げられる。

【００５０】例えば、車両所有者が携帯電話等から、エアコンを起動するための指令を車載ＬＡＮ１０内の上記エアコンＥＣＵ２５に入力して、エアコンをリモコン操作する場合のアクセスが挙げられる。また、利用者が電話回線を通じて楽曲データを取得して、これを車両内のオーディオＥＣＵ３３にて再生させる場合のアクセス等も考えられる。この他に、利用者が電話回線を通じて外部センタから、車載ＬＡＮ内の各ＥＣＵ１１～３７にて動作するプログラムを取得し、これをＥＣＵ１１～３７にインストールして、プログラムを新規に書き込んだり、更新したりする場合のアクセスが考えられる。

【００５１】以上には、通信部４０内の各無線機４１，４３，４５，４７について説明したが、当該車内通信システム１においては、外部から配信先（即ち、アクセス先）の指示がない通信データを通信部４０にて受信する場合が考えられる。したがって、このような場合の対処を施す場合には、例えば、各無線機４１～４７が、配信先の指示のない特定種のデータに関して、配信先に関する情報を通信データに付与し、これをゲートウェイＥＣＵ５０に送信するように通信部４０を構成すればよい。例えば、テレビ信号を受信した場合に、配信先をオーディオＥＣＵ３３に指定するなどである。

【００５２】この他、外部装置接続部４９は、車両診断を行うためのサービスツール５や、ＥＣＵ内のプログラムを更新するためのサービスツール５等の車外装置を、

車載ＬＡＮ１０に接続するためのコネクタから構成されており、サービスツール５が接続されると、サービスツール５をゲートウェイＥＣＵ５０に接続する構成となっている。

【００５３】また、ゲートウェイＥＣＵ５０は、通信部４０と、車載ＬＡＮ１０と、に接続されており、車載ＬＡＮ１０内の各ＥＣＵ１１～３７と車外装置３との間のデータ通信を中継するための構成を有している。例えば、ゲートウェイＥＣＵ５０は、所謂ルーティング機能を有しており、車載ＬＡＮ内の各系ネットワーク内のＥＣＵから車載ＬＡＮ内の他のネットワーク内のＥＣＵへのアクセスを中継する。具体的に例えば、ボディ系ネットワーク内のＥＣＵから制御系ネットワーク内のＥＣＵへのアクセスの要求があると、ボディ系ネットワーク内のＥＣＵからの通信データを、制御系ネットワーク内のＥＣＵに送信する。

【００５４】また、本発明の係る特徴として、このゲートウェイＥＣＵ５０は、通信部４０が受信した通信データを取得すると、自身のＣＰＵにて、図２に示すメインルーチンを実行する。図２は、ゲートウェイＥＣＵ５０で実行されるメインルーチンを表すフローチャート、図３は、そのメインルーチンにて呼び出されるプログラム転送処理を表すフローチャート、図４（ａ）は、そのプログラム転送処理にて呼び出される個別認証処理を表すフローチャート、図５は、アクセス制限処理を表すフローチャートである。

【００５５】ゲートウェイＥＣＵ５０は、まずＳ１１０にて、通信データの配信先を、その通信データから読み取り、これに基づいて、配信先（即ち、アクセス先）が、自身の記憶媒体（本実施例では、メモリ）に記憶された車内搭載機器リストにリストアップされているものであるかどうか判断する（Ｓ１２０）。尚、ここでいう車内搭載機器リストとは、車載ＬＡＮ１０に接続されたＥＣＵ１１～３７に関するリストのことである。

【００５６】ここで、通信データの配信先が車内搭載機器リストに登録されていないと判断すると、ゲートウェイＥＣＵ５０は、Ｓ１２５にてアクセス制限処理（詳しくは後述）を実行した後に、当該処理を終了する。一方、通信データの配信先が車内搭載機器リストに登録されていると判断すると、ゲートウェイＥＣＵ５０は、続くＳ１３０にて、その通信データが、車載ＬＡＮ１０内のＥＣＵにて動作するプログラムの書込要求に関する情報又は車両内の制御システムを的確に動作させるための適合定数の書込要求に関する情報を含む通信データであるかどうかを判断する。尚、ここでいう適合定数の書込要求とは、例えば、エンジン点火時期マップの書換要求等のことである。

【００５７】そして、通信データに、プログラム又はパラメータの書込要求に関する情報が含まれていると判断すると、ゲートウェイＥＣＵ５０は、次にＳ１４０にてプログラム転送処理（図３）を実行する。尚、以降の処理については、プログラムの書込要求についてのみ説明するが、これらの処理は、適合定数の書込要求であった場合においても、同様の手順で行われる。

【００５８】プログラム転送処理に移行すると、ゲートウェイＥＣＵ５０は、まずＳ１４１にて、通信部４０を介してそのプログラムの書込要求を送信してきた車外装置３に、自身宛に第一の認証情報としてパスワードを送信するように要求し、車外装置３からパスワードを取得する。

【００５９】続いて、ゲートウェイＥＣＵ５０は、Ｓ１４３にて、そのパスワードが、自身（ゲートウェイＥＣＵ５０）に予め登録されたパスワードと一致するかどうかを判断する。尚、このパスワードに関しては、例えば、製品出荷時に生産者が当該ゲートウェイＥＣＵ５０にそのゲートウェイＥＣＵ５０固有のパスワードを登録しておけばよい。

【００６０】そして、Ｓ１４３にてパスワードが正しくない（つまり、取得したパスワードと、予め登録されているパスワードが一致しない）と判断すると、ゲートウェイＥＣＵ５０は、処理をＳ１６９に移行して、アクセス制限処理（図５）を実行した後に当該処理を終了し、Ｓ１４３にてパスワードが正しいと判断すると、処理をＳ１４５に移行してプログラムを車外装置３から通信部４０を介して取得し、自身のメモリ内に一時格納する。

【００６１】続いて、ゲートウェイＥＣＵ５０は、Ｓ１５０にて個別認証処理（図４）を実行する。個別認証処理に移行すると、ゲートウェイＥＣＵ５０は、まずＳ１５１にて、車外装置３がプログラムの書込対象としている車載ＬＡＮ１０内のＥＣＵ（以下、「書込対象ＥＣＵ」と表現する。）に、プログラムの受信を要求する。

【００６２】このようにゲートウェイＥＣＵ５０がプログラムの受信を要求すると、要求を受けた書込対象ＥＣＵは、図４（ｂ）にフローチャートを示すプログラム受信処理を実行する。以下、図４（ａ）に示すゲートウェイＥＣＵ５０が実行する個別認証処理の詳細と、図４（ｂ）に示すプログラム受信処理の詳細を並行して説明することにする。

【００６３】プログラムの受信要求を受けた書込対象ＥＣＵは、まずＳ３１０にて、プログラムの書込要求をしてきた車外装置３が、プログラムの書込を予め許可された車外装置３であるか否かを判別するために、上記第一の認証情報とは異なる第二の認証情報を書込要求元の車外装置３に要求する。

【００６４】例えば、認証方式として共通鍵方式（ＤＥＳ方式等）を採用した場合、書込対象ＥＣＵは、Ｓ３１０にて、乱数ｒを生成し、これを一旦、自身のメモリ内に記憶すると共に、この乱数ｒを認証情報の要求と共に車外装置３側に送信して、車外装置３に対して、乱数ｒを共通鍵Ｋで暗号化したものを認証情報として送り返す

ように指示する。

【００６５】尚、この認証情報の要求を車外装置３に行う際には、一度ゲートウェイＥＣＵ５０が、その要求情報を書込対象ＥＣＵから取得し、これを通信部４０を介して車外装置３に転送する（Ｓ１５３）。また、ゲートウェイＥＣＵ５０は、この認証情報の要求に対する応答結果として車外装置３から認証情報を取得すると、Ｓ１５５にて、これを書込対象ＥＣＵに転送する。

【００６６】一方、書込対象ＥＣＵは、ゲートウェイＥＣＵ５０を介して、車外装置３から認証情報を取得すると（Ｓ３２０）、これを、自身のメモリ内に記憶された認証情報と照合する（Ｓ３３０）。そして、照合結果に基づき、車外装置３の認証が成功したか否かを判断し（Ｓ３４０）、認証が成功していれば、認証成功をゲートウェイＥＣＵ５０に通知し（Ｓ３５０）、認証が成功しなければ、認証が失敗したことを通知する（Ｓ３５５）。

【００６７】ここで、上記共通鍵方式の認証を行う場合の例を具体的に説明すると、書込対象ＥＣＵは、車外装置３から取得した認証情報を、共通鍵Ｋで復号して、この復号化した認証情報が、Ｓ３１０にて生成した乱数ｒと一致するか否か判断し、一致すれば、車外装置３が予めプログラムの書込を許可された車外装置であるとして（Ｓ３４０でＹｅｓ）、その車外装置３の認証が成功したことを通知する。

【００６８】一方、ゲートウェイＥＣＵ５０は、Ｓ１５７にて書込対象ＥＣＵから認証結果（認証成功の通知もしくは認証失敗の通知）を受信すると、当該個別認証処理を終了して、プログラム転送処理（図３）のＳ１６１にて、書込対象ＥＣＵでの認証が成功したか否かを判断する。

【００６９】つまり、ゲートウェイＥＣＵ５０は、書込対象ＥＣＵから認証失敗の通知を受けると、Ｓ１６１でＮｏと判断して、処理をＳ１６９に移し、書込対象ＥＣＵから認証成功の通知を受けると、Ｓ１６１でＹｅｓと判断して、処理をＳ１６３に移す。

【００７０】そして、Ｓ１６３において、ゲートウェイＥＣＵ５０は、一時記憶しておいたプログラムを、書込対象ＥＣＵに送信する。尚、これに対応して、書込対象ＥＣＵは、ゲートウェイＥＣＵ５０から転送されてきたプログラムを受信して、そのプログラムを、自身のメモリ内に実行可能な状態にて、記憶する（Ｓ３６０）。

【００７１】また、ゲートウェイＥＣＵ５０は、書込対象ＥＣＵがプログラムを記憶し終わると、Ｓ１６５にて、書込対象ＥＣＵが正しくプログラムを記憶したかどうかを検証する。例えば、ゲートウェイＥＣＵ５０は、自身が転送したプログラムの内容と、書込対象ＥＣＵがメモリ内に記憶したプログラムとが同一内容であるかどうか照合することにより、書込対象ＥＣＵが正しくプログラムを記憶したかどうかを検証する。

【００７２】そして、正しくプログラムが記憶されていれば、自身のメモリ内から、Ｓ１６３にて送信したプログラムを破棄して（Ｓ１６７）、当該処理を終了し、正しくプログラムが記憶されていなければ（Ｓ１６５でＮｏ）、再度自身のメモリ内に記憶されたプログラムを読み出し、これを書込対象ＥＣＵに送信する（Ｓ１６３）。尚、プログラムの書込が複数回に渡ってうまくいかない場合には、プログラムの書込を中止して、当該処理を終了させればよい。

【００７３】次に、Ｓ１３０（図２参照）にて、ゲートウェイＥＣＵ５０が通信データをプログラム、適合定数の書込要求ではないと判断した（Ｓ１３０でＮｏ）場合の処理について説明する。図２に示すように、ゲートウェイＥＣＵ５０は、Ｓ１３０にてＮｏと判断すると、続くＳ１７０にて、通信データの配信先（アクセス先）が、ＡＶＣ系ネットワークに接続されたＡＶＣ系ＥＣＵ３１～３７であるか否かを判断する。

【００７４】ここで、配信先がＡＶＣ系ＥＣＵ３１～３７であると判断すると（Ｓ１７０でＹｅｓ）、ゲートウェイＥＣＵ５０は、Ｓ１７５にて、通信データを配信先のＡＶＣ系ＥＣＵに配信する。一方、配信先がＡＶＣ系ＥＣＵ３１～３７ではないと判断すると（Ｓ１７０でＮｏ）、ゲートウェイＥＣＵ５０は、通信部４０を介して、そのデータを送信してきた車外装置３に、当該ＥＣＵ宛へパスワードを送信するように要求して、車外装置３から認証情報としてのパスワードを取得する（Ｓ１８０）。

【００７５】続いて、ゲートウェイＥＣＵ５０は、Ｓ１９０にて、パスワードが、自身に予め登録されたパスワードと一致するかどうかを判断することにより、取得したパスワードが正しいか否か判断する。尚、ゲートウェイＥＣＵ５０は、車外装置３から取得したパスワードを、上述したプログラム転送処理のＳ１４３で照合するのに用いたのと同じパスワードで照合する構成にされていてもよいし、別のもので照合するように構成されていてもよい。この場合には、ゲートウェイＥＣＵ５０に、予めＳ１４３の照合の際に用いるパスワードと、Ｓ１９０の照合の際に用いるパスワードを、両方記憶させておくことになる。

【００７６】そして、パスワードが正しいと判断すると（Ｓ１９０でＹｅｓ）、ゲートウェイＥＣＵ５０は、データを配信先のＥＣＵに送信し（Ｓ２００）、パスワードが正しくないと判断すると（Ｓ１９０でＮｏ）、Ｓ１９５にてアクセス制限処理を実行して、当該処理を終了する。

【００７７】尚、このアクセス制限処理において、ゲートウェイＥＣＵ５０は、図５に示すように動作する。即ち、ゲートウェイＥＣＵ５０は、Ｓ４１０にて、同一の車外装置３から当該ゲートウェイＥＣＵ５０に、一定時間内でｎ回（例えば３回）以上のアクセスがあったか否

か判断して、ｎ回以上のアクセスがなければ（Ｓ４１０でＮｏ）、Ｓ４２０にて、認証に失敗した異常なアクセスが車外装置３よりあったことを通信部４０の対応する無線機４１～４７に送信（これに対応する無線機４１～４７の動作については後述）して、当該処理を終了する。

【００７８】一方、ｎ回以上のアクセスがあった場合には（Ｓ４１０でＹｅｓ）、対応する無線機４１～４７にその車外装置３からのアクセスを禁止するように通知して（Ｓ４３０）、無線機４１～４７に、同一アクセス元の車外装置３からの通信データを、ゲートウェイＥＣＵ５０に二度と送らないようにさせて、当該処理を終了する。

【００７９】また、このアクセス制限処理の上記各通知を受ける本実施例の各無線機４１～４７は図６に示すようなアクセス制御処理を実行して、車外装置３からのアクセスを制御する。尚、図６は、アクセス制御処理を表すフローチャートである。無線機４１～４７は、復調回路から、復調結果としての通信データを取得すると、通信データに含まれる送信元の車外装置３に関する情報を取得して、その送信元を識別し（Ｓ５１０）、Ｓ５２０にて、送信元がアクセス禁止リストにあるか否か判断する。尚、このアクセス禁止リストは、ゲートウェイＥＣＵ５０からアクセス禁止の通知を受ける度に、無線機４１～４７が逐次更新していくものであり、無線機４１～４７は、自身のメモリ内に、アクセス禁止の対象となった車外装置３を登録したアクセス禁止リストを保有している。

【００８０】このＳ５２０において通信データの送信元がアクセス禁止リストにあると判断すると、無線機４１～４７は、続くＳ５４０にて、送信元の車外装置３のゲートウェイＥＣＵ５０へのアクセスを拒否する。つまり、無線機４１～４７は、その送信元から受信した通信データをゲートウェイＥＣＵ５０に送信することなく破棄する。

【００８１】一方、Ｓ５２０において、通信データの送信元がアクセス禁止リストにないと判断すると、無線機４１～４７は、続くＳ５３０にて、その送信元が異常アクセスを受けてから一定時間経過したものであるか否かを判断する。尚、ここでの一定時間は、ゲートウェイＥＣＵ５０がＳ４１０にてｎ回以上のアクセスがあったか否かを判断する際の時間より十分短い時間に設定されている。

【００８２】ここで、異常アクセス後一定時間が経過していないと判断すると、無線機４１～４７は、Ｓ５４０に移動して、送信元の車外装置３のゲートウェイＥＣＵ５０へのアクセスを拒否する。一方、異常アクセス後一定時間が経過しているか、異常アクセスの通知をうけていないと判断すると、処理をＳ５５０に移して、通信データをゲートウェイＥＣＵ５０に送信する。

【００８３】以上、本実施例の車内通信システム１について説明したが、この車内通信システム１においては、ゲートウェイＥＣＵ５０が、車外装置３に接続される通信部４０と、車載ＬＡＮ１０との間の通信を中継する際に、必要に応じて車外装置３が車載ＬＡＮ１０の各ＥＣＵ１１～３７へのアクセス（即ち、各ＥＣＵとのデータ通信）を許可された車外装置かどうかを、パスワードを取得することにより確認するので、車載ＬＡＮ１０内の各ＥＣＵ１１～３７への不正なアクセスを防止することができる。また、このような構成にすることにより、個別のＥＣＵだけで車外装置３を認証する場合よりも、外部から不正なアクセスを一層防止することができるし、そのようなシステムを安価に構成することができる。この他、車内通信システムにおける配線を少なくすることができる。

【００８４】尚、本実施例の車内通信システム１では、通信データがプログラム、適合定数の書込要求に関するものでなく、通信データの配信先（アクセス先）が外部から取得した情報を車両乗員に報知するためのＡＶＣ系ＥＣＵ（ＡＶＣ系ネットワークに接続されたＥＣＵ３１～３７）である場合に、車外装置３の認証を行わない事にしている。

【００８５】なぜならば、ＡＶＣ系ＥＣＵ３１～３７への通信データである限り、その通信データに悪意で作為がなされていたとしても、その通信データが車両の走行に関する安全性に影響を与えることがないからである。また、ＡＶＣ系ＥＣＵへのアクセスが外部から頻繁に行われることを考慮にいれれば、いちいち車外装置３の認証を行うと、ゲートウェイＥＣＵ５０への処理負荷が高くなってしまうからである。尚、勿論、必要があれば各ＥＣＵにて個別に認証を行っても構わない。

【００８６】一方、通信データの配信先がＡＶＣ系ＥＣＵ以外のＥＣＵである場合（換言すると、制御系ネットワーク、ボディ系ネットワークに接続されたＥＣＵ１１～２５である場合）には、少なくとも、パスワード等による車外装置３の認証を一回行うようにしている。なぜならば、制御系ネットワークや、ボディ系ネットワークに接続される各ＥＣＵは車両制御にかかわるＥＣＵであるため、不正にこれらのＥＣＵがいたずらされないようにし、車両の走行安全性を確保することが必要だからである。

【００８７】また特に、本実施例の車内通信システム１においては、通信データがプログラム、適合定数の書込要求に関するものである場合、配信先のＥＣＵの種類にかかわらず、パスワード等による第一の認証に加えて第二の認証を行うことにより、車外装置３のアクセスをより厳しく制限している。したがって、本実施例の車内通信システム１においては、ＥＣＵにて動作するプログラムや、車両制御に係わる適合定数が不正に書き換えられてしまうなどの事態を防止することができる。

【００８８】この他、この車内通信システム１においては、認証に失敗することの多い車外装置３からのアクセスをｎ回の認証失敗をもって禁止して、通信部４０にて車外装置３からの通信データをゲートウェイＥＣＵ５０に入力しないようにしているため、不正アクセスによってゲートウェイＥＣＵ５０の処理負荷が高まってしまうなどの問題を解消することができる。

【００８９】ここで、以上に説明した本実施例の車内通信システム１と本発明の車内通信システムとの関係は以下のようになっている。まず、本発明の車両用中継装置は、本実施例のゲートウェイＥＣＵ５０に相当し、本発明の情報系装置は、上記ＡＶＣ系ネットワークに接続されたＡＶＣ系ＥＣＵ３１～３７に相当し、本発明の制御系装置は、上記制御系ネットワークもしくはボディ系ネットワークに接続された各ＥＣＵ１１～２５に相当する。また、車外装置のアクセス要求は、車外装置３が通信部４０に通信データを送信する動作に相当する。

【００９０】そして、本発明の第一識別手段は、ゲートウェイＥＣＵ５０がＳ１１０で把握した配信先に基づき、Ｓ１７０にて、配信先が情報系装置としてのＡＶＣ系ＥＣＵであるか否かを判断する動作に相当し、第一認証手段は、ゲートウェイＥＣＵ５０がＳ１８０にて第一の認証情報としてのパスワードを取得し、Ｓ１９０にてパスワードが正しいか否か判断する動作に相当する。また、第一配信手段は、ゲートウェイＥＣＵ５０がＳ１７０でＹｅｓと判断した時に実行するＳ１７５と、Ｓ１９０でＹｅｓと判断した時に実行するＳ２００の処理に相当する。

【００９１】この他、本発明の第二識別手段は、ゲートウェイＥＣＵ５０が実行するＳ１３０での処理動作に相当し、第二認証手段は、ゲートウェイＥＣＵ５０がアクセス要求をプログラム等の書込要求ではないと判断した際にステップをＳ１７０に移行する一方で、アクセス要求がプログラム等の書込要求であった場合に、Ｓ１４０～Ｓ１６１の処理を実行する動作に相当する。また、第二配信手段は、ゲートウェイＥＣＵ５０がＳ１６１の判断結果に基づき、ステップをＳ１６３に移行して、通信データ（プログラム等）をＥＣＵに送信する動作に相当する。

【００９２】以上、本発明の実施例について説明したが、本発明の車両用中継装置及び車内通信システムは、上記実施例に限定されるものではなく、種々の態様を採ることができる。例えば、上記実施例においては車外装置３の認証をまずパスワードにて行う構成としたが、その他の認証方法にて車外装置３を認証してもよい。共通鍵方式等のより信頼性の高い認証方法で車外装置３を認証すれば、認証時間が長くなる場合もあるが、より確実に車載ＬＡＮ１０内のＥＣＵへの不正アクセスを防止することができる。

【００９３】この他、プログラム等の書込要求を受信した場合においては、異なる認証方法で、車外装置３を２回認証する構成としたが、これらの書込に関する安全性を確保するためには、信頼性の高い認証方法で認証を３回以上行ってもよいし、一度だけ、信頼性の非常に高い認証方法で車外装置３を認証するように当該システムを構築してよい。

【図面の簡単な説明】

【図１】　本実施例の車内通信システム１の構成を表すブロック図である。

【図２】　ゲートウェイＥＣＵ５０が実行するメインルーチンを表すフローチャートである。

【図３】　ゲートウェイＥＣＵ５０が実行するプログラム転送処理を表すフローチャートである。

【図４】　ゲートウェイＥＣＵ５０が実行する個別認証処理を表すフローチャート（ａ）と、書込対象ＥＣＵが実行するプログラム受信処理を表すフローチャート（ｂ）である。

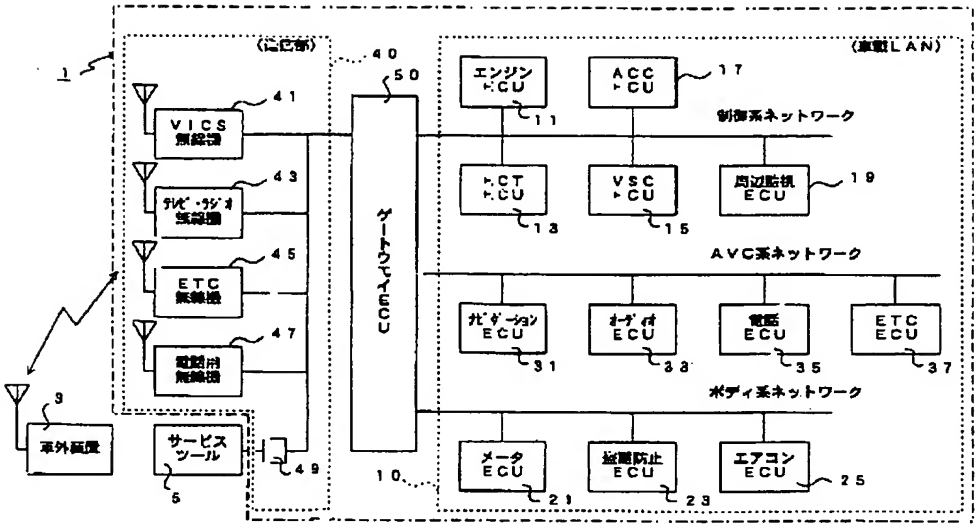
【図５】　ゲートウェイＥＣＵ５０が実行するアクセス制限処理を表すフローチャートである。

【図６】　各無線機４１～４７が実行するアクセス制御処理を表すフローチャートである。

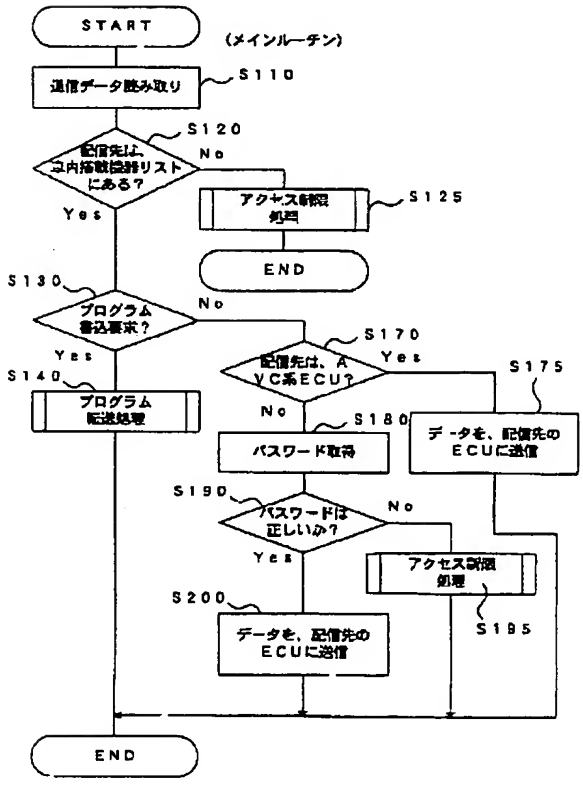
【符号の説明】

１…車内通信システム、３…車外装置、１０…車載ＬＡＮ、１１～３７…ＥＣＵ、４０…通信部、４１，４３，４５，４７…無線機、４９…外部装置接続部、５０…ゲートウェイＥＣＵ

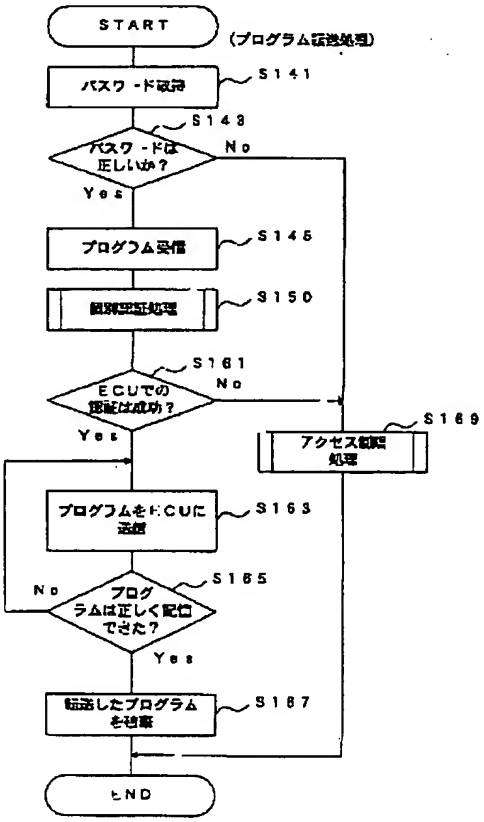
【図1】


(自車両)
(車載LAN)
1
40
50
41
VICS 無線機
43
ETC 無線機
45
47
9
車外装置
サービス ツール
5
49
10
ゲートウェイCOM
エンジン ECU
11
ACC ECU
17
制御系ネットワーク
ECT ECU
13
VSC ECU
15
周辺監視 ECU
19
AVC系ネットワーク
ナビゲーション ECU
31
オーディオ ECU
33
電話 ECU
35
ETC ECU
37
ボディ系ネットワーク
メータ ECU
21
盗難防止 ECU
23
エアコン ECU
25

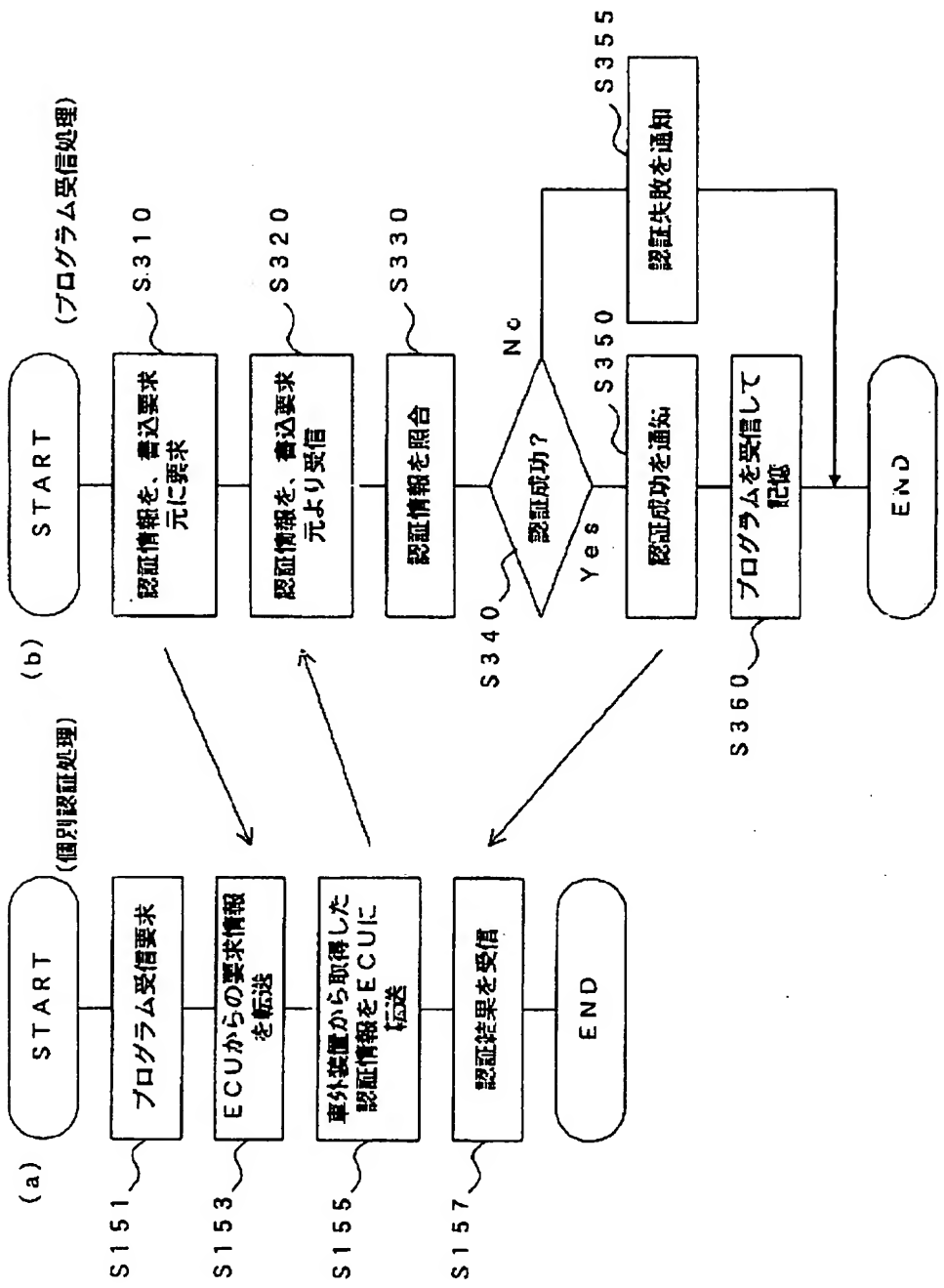
【図2】


START
(メインルーチン)
通信データ読み取り
S110
S120
記憶先は、車内搭載機器リストにある?
No
Yes
アクセス制限処理
S125
END
S130
プログラム書込要求?
No
Yes
S140
プログラム転送処理
S170
記憶先は、AVC系ECU?
Yes
No
S175
データを、記憶先のECUに送信
S180
パスワード取得
S190
パスワードは正しいか?
No
Yes
アクセス制限処理
S195
S200
データを、記憶先のECUに送信
END

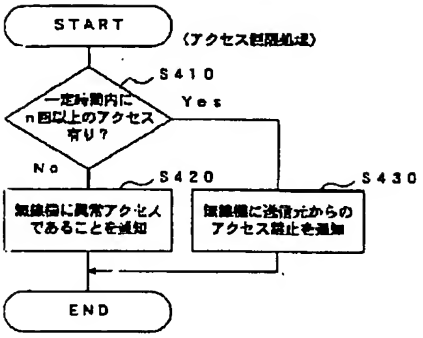
【図3】


START
(プログラム転送処理)
パスワード取得
S141
S143
パスワードは正しいか?
No
Yes
プログラム受信
S145
暗証照合処理
S150
S161
ECUでの認証は成功?
No
Yes
S169
アクセス制限処理
プログラムをECUに送信
S163
S165
プログラムは正しく記憶できた?
No
Yes
転送したプログラムを破棄
S167
END

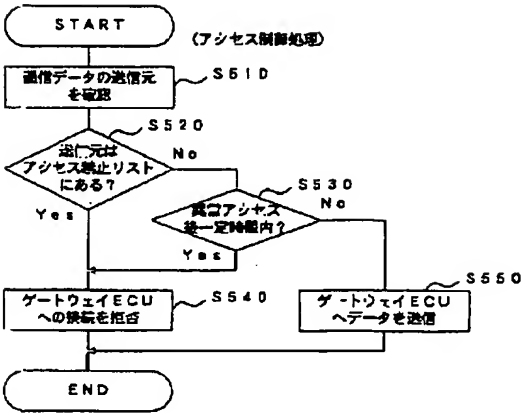
【図4】


(a)
(個別認証処理)
START
プログラム受信要求
ECUからの要求情報を転送
車外装置から取得した認証情報をECUに転送
認証結果を受信
END
S151
S153
S155
S157
(b)
(プログラム受信処理)
START
認証情報を、書込要求元に要求
認証情報を、書込要求元より受信
認証情報を照合
認証成功?
No
Yes
認証失敗を通知
認証成功を通知
プログラムを受信して記憶
END
S310
S320
S330
S340
S350
S355
S360

【図5】


START
(アクセス制限処理)
S410
一定時間内にn回以上のアクセス有り?
Yes
No
S420
無線機に異常アクセスであることを通知
S430
無線機に送信元からのアクセス禁止を通知
END

【図6】


START
(アクセス制御処理)
通信データの送信元を確認
S510
S520
送信元はアクセス禁止リストにある?
No
Yes
S530
異常アクセス後一定時間内?
No
Yes
S540
ゲートウェイECUへの接続を拒否
S550
ゲートウェイECUへデータを送信
END